紫光比威
UNIS BITWAY

用户手册

BitStream3224TM+

智能型快速以太网交换机



清华比威
TSINGHUA BITWAY



用户手册

BitStream3224TM+

智能型快速以太网交换机

BitStream3224TM+

Rev1.0



总公司	**深圳公司**
清华紫光比威网络技术有限公司	**深圳市清华紫光比威网络技术有限公司**
北京市西城区金融大街 35 号国企大厦	**深圳市高新技术产业园南区清华大学研究院**
C **座** 12 **层**	4 **楼** C **区东**
邮编：100032	**邮编：**518057
电话：（010）88092299	**电话：（**0755）26957188
传真：（010）88092298	**传真：（**0755）26957108
Internet：support@bit-way.com	

目 录

前 言 **1**

第一部分 **2**

第一章 关于本款交换机 **6**

概述 6
硬件描述 8
特性和优点 13

第二章 网络规划 **15**

交换简介 15
应用举例 16
连接规则 18
应用要点 21

第三章 安装交换机 **23**

选择安装位置 23
箱内物品 23
安装 23
连接电源 28

第四章 网络连接 **29**

连接网络设备 29
双绞线设备 29
光纤设备 32

附录 A 疑难解答 **35**

通过指示灯诊断 35
电源及冷却系统故障 35
安装 36
IN-BAND 访问 36

附录 B 线缆 **37**

规格 37
双绞线和管脚分配 38
控制台口管脚分配 40

附录 C 规格 **43**

物理特性 43
管理特性 44
标准 45
遵从 45

第二部分 **47**

第一章 初始配置 **48**

连接交换机 48
基本配置 51
管理系统文件 57
系统默认值 58

第二章 配置交换机 **62**

使用 WEB 界面 62

操作 WEB 浏览器界面 62
面板显示 64
主菜单 64
基本配置 64
配置用户认证 70
管理固件 74
重设系统 77
显示网桥扩展性能 78
激活或禁用 GVRP（全局设置） 80
显示激活就硬件/软件版本 80
端口配置 83
配置端口镜像 90
地址表设置 91
生成树算法的配置 95
VLAN 的配置 104
配置私有 VLAN 117
服务类别的配置 123
端口 TRUNK 配置 125
配置 SNMP 127
显示端口统计表 130
速率限制配置 132

第三章 命令行界面 135

使用命令行界面 135
输入命令 137
命令组 144
常规命令 145

FLASH/FILE 命令 151
系统管理命令..... 158
认证命令..... 169
SNMP 命令..... 174
行命令..... 180
LOGIN..... 182
IP 命令 190
接口命令..... 195
速率限制命令..... 209
地址表命令..... 210
生成树命令..... 215
VLAN 命令..... 223
私有 VLAN 命令..... 233
GVRP 和桥路扩展命令 239
优先级命令..... 245
镜像端口命令..... 246
端口聚合命令..... 248
附录 A 疑难解答..... 251
常见故障..... 251
通过串口升级固件..... 251
附录 B 管脚分配..... 255
控制口管脚分配..... 255

前 言

感谢您购买了清华比威的 BitStream 3224TM+快速以太网交换机。

本手册说明如何安装和使用 BitStream 3224TM+。这款交换机支持10/100Mbps 速率和半/全双工模式的自动协商，支持端口线性自适应、802.1Q VLAN 划分和端口干路连接（Trunking）等技术。

为了能充分利用本手册,您应当理解 IEEE 802.3 以太网标准、100BASE-TX 快速以太网和局域网（LAN）等网络概念。有关这些概念的更多内容，请参见附录。

在本手册中，您将看到安装和配置两部分内容：

- 第一部分　安装手册
- 第二部分　管理手册

第一部分

BitStream3224TM+

安装手册

兼容性

FCC – A级

此设备产生、使用和能辐射无线频率能量，如果按照手册指示安装和使用，可能引起与无线通信的冲突。它已经通过测试，与计算机设备所要求FCC规则的A级和B级的15部分都相符合。它可以防止冲突，给商业环境提供一个合理的保护。在居民区运行此设备可能引起干扰，用户可能需要自己花钱采取措施防止正这些干扰。您必须注意任何没有经过所负责部门任何修改和更正都无效。

您可以使用非屏蔽的RJ-45连接头双绞（UTP）电缆——支持10 Mbps连接的3类或更大，支持100 Mbps连接的5类。使用50/125 或62.5/125微米的多模光纤电缆，或带有SC-type连接头的9/125微米的单模光纤电缆。

警告: 1. **当操作此装备时，使用一条防静电的皮带或其它适当的方式来防止静电。**

2. **当把集线器连接到电源插座时，保证三相插座要有地线，以阻止电磁波的干扰。**

加拿大行业标准A级

这个数字仪器没有超过来自于此仪器的广播噪音发射的A级限定，在引起干扰的授名为“数字仪器”（通信部的ICES-003）的装置标准中测定。

日本VCCI A 级

EC 一致声明 —— A级

这个信息技术装置符合委员会所提出的89/336/EEC要求，接近所有成员国的定律：电磁兼容性，73/23/EEC对某些电器设备电压的限制，修改指示93/68/EEC。可以参考下面的标准来评估是否符合这些指示：

RFI **辐射**:

- A**级限定依据**EN 55022:1998
- **支持辐射的**A**级限定依据**EN 61000-3-2 1995

限定电压波动和在低电压提供系统闪烁依据 EN 61000-3-3/1995

绝缘:

- **产品系列规格依据**EN 55024:1998
- **静电释放依据**EN 61000-4-2:1995

(**接触放电**: ± 4 kV, **空气放电**: ± 8 kV)

- **无线电频率磁场依据**EN 61000-4-3:1996

(80 – 1000 MHz **，** 1 kHz AM 80% **调制**: 3 V/m)

- **电的快速/瞬时脉冲依据**EN 61000-4-4:1995

(AC/DC **电源提供**: ± 1 kV, **数据/信号线**: ± 0.5 kV)

- **电涌免疫测试依据**EN 61000-4-5:1995

(AC/DC Line to Line: ± 1 kV, AC/DC Line to Earth: ± 2 kV)

- **由无线电频率引起的对导电干扰的免疫：**EN 61000-4-6:1996

(0.15 – 80 MHz **，** 1 kHz AM 80%**调制**: 3 V/m)

- **电源频率磁场免疫测试依据**EN 61000-4-8:1993 (1 A/m**频率为**50 Hz)
- **电压倾斜**, **短时中断和电压变化免疫测试依据**EN 61000-4-11:1994 (>95% **减少** @10 ms, 30% **减少**@500 ms, >95% **减少**@5000 ms)

LVD

- EN 60950 (A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)

Australia AS/NZS 3548 (1995) – Class A



第一章 关于本款交换机

概述

本款交换机是理想的解决方案,在多住处或多出租住宅(简称 MDU/MTU)如公寓住宅区、商务建筑或酒店中，它能使单独的用户共享因特网访问。此款交换机为用户提供了配有带宽的连接，各用户间的端口对端口隔离，保证安全。在 MDU/MTU 中，能级联多达 24 个其他交换机，每台交换机可以为多达 24 个用户提供宽带因特网访问。

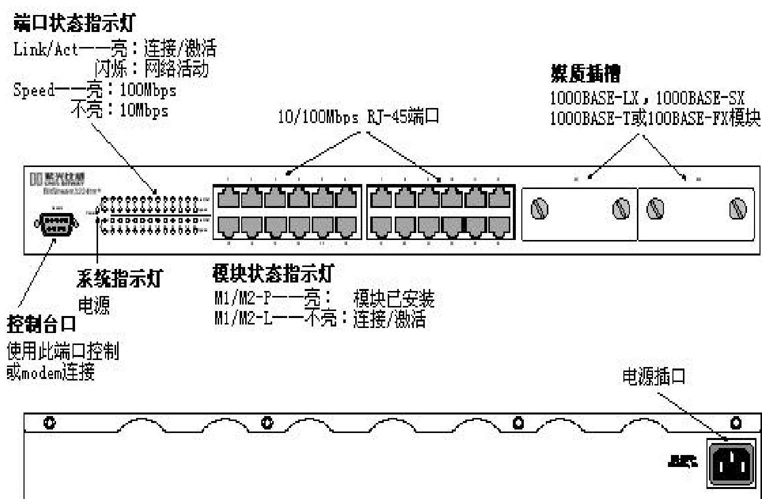


图 1-1 前后面板

交换机机构

交换机前面板上有24个10/100Mbps快速以太网端口。每个端口能提供专门的链接直接到终端用户PC，或在终端用户前提连接另一个以太网交换机/集线器，用做共享链接。交换机对每个终端用户链接提供了100Mbps全双工的配置带宽，从而完全消除拨号上网的瓶颈。对于所有端口的连接，交换机的9.6 Gbps带宽容量足以应付最苛刻的环境。

自适应用于选择最佳的传输速率和传输模式。即使在超负载在情况下，仍能维持存储和转发交换以及流量控制、最大的数据完整性。

此款交换机的前面板有两个插槽，用于插1000BASE-LX，1000BASE-SX，1000BASE-T或100BASE-FX模块。使用这些模块就可完成交换机间的级联。通过光纤上连模块就能直接连接因特网服务供应商（ISP）。100BASE-LX支持1Gbps连接远达5千米；用单模光纤电缆，100BASE-FX支持100Mbps连接，远达20千米。

管理选项

此款交换机的LED指示灯能“时刻”监控网络和端口状态。它也包括一个管理代理，使用代理的内嵌管理软件或通过SNMP应用，你就能配置或监控交换机。若为了管理交换机，你能直接连接RS-232控制台端口（out-of-band），使用Telnet或基于Windows的网络管理软件，通过网络连接（in-band）管理交换机。

管理代理提供大范围的高级性能。基于端口的VLAN提供数据流安全性和网络带宽的有效使用。QoS优先列队确保通过交换机传输时多媒体数据时的最小耽搁。流量控制消除了数据包的丢失（由于端口饱和引起的瓶颈导致数据包丢失）。端口安全性从交换机过滤掉多余的数据流。

如要获取详细描述，请参看管理手册。

VLAN

如果在交换机上配置多个 VLAN（虚拟局域网），每个 VLAN 就像一台包含多个端口的“逻辑交换机”。每个逻辑交换机就是一个隔离的广播域，就像虚拟的局域网一样。物理交换机的转发、过滤和涌出行为和操作同样适用于 VLAN 所定义的逻辑交换机；如：数据包只能转发或涌出到指定的 VLAN 端口。在分离的 VLAN 端口之间没有通信，除非 VLAN 连接了外接路由器或第三层交换机才能实现各 VLAN 之间的通信。

硬件描述

RJ-45 端口

交换机有 24 个 10BASE-T / 100BASE-TX RJ-45 端口。所有的端口都支持自动 MDI/MDI-X 操作，因此你能使用直通线完成所有的网络连接到 PC 或服务器，或到其他交换机或集线器。（参看附录 B）

每个端口都支持 IEEE802.3x 自适应，因此最适宜的传输模式（半或全双工），和数据速率（10 或 100Mbps）能被自动选择（如果这个特性也被所连设备支持）。如果连接到这些端口的设备不支持自适应，那么端口

将发送正确的速度，但是传输模式将默认为半双工。这些端口的发送和接收带宽受到一个可调整的 8 层阈值的限制（参看第二章中的“带宽配置连接”）。

每个端口也支持流量控制自适应，因此交换机能自动防止端口缓存变为饱和。

状态 LED

交换机的显示面板能显示关键系统和端口的状态，便于发现并解决故障。下表描述了位于前面板的 LED 指示灯。

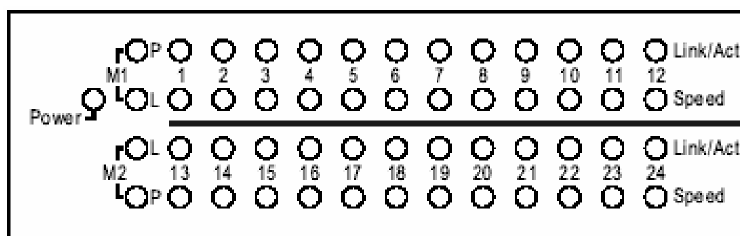


图 1-2 端口和系统 LED

端口状态 LED		
LED	**条件**	**状态**
端口 1-24		
Link	亮	端口已建立有效网络连接
	闪	显示端口有网络活动
Speed	亮	端口以 100Mbps 的速率操作
	不亮	端口以 10Mbps 的速率操作

模块端口		
M1/M2-P	亮	此端口已安装模块
	不亮	此端口没有安装模块
M1/M2-L	亮	模块已建立有效网络连接，端口被激活
	闪	模块没有建立有效网络连接，或端口禁用

系统状态 LED		
LED	**条件**	**状态**
Power	亮	交换机通电

可选的媒质扩展模块

可选的 1000BASE-T 模块

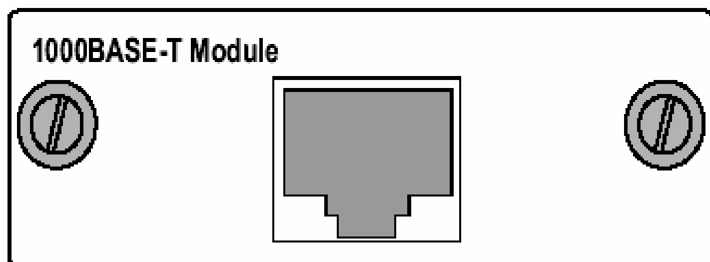


图 1-3 单端口 1000BASE-T 模块

使用 5 类或 5e 双绞线你能连接 100 米远的另一个设备。1000BASE-T 模块以 10/100/1000Mbps 的速率操作。1000Mbps 速率时，它支持全双工、

速度自适应和流量控制。10/100Mbps 速率时，它支持全或半双工模式、速度自适应和流量控制。注意你首先应该测试电缆的安装是否符合 IEEE802.3ab 标准。参看附录 B 中" 1000BASE-T 电缆要求"。

可选的 1000BASE-SX 模块

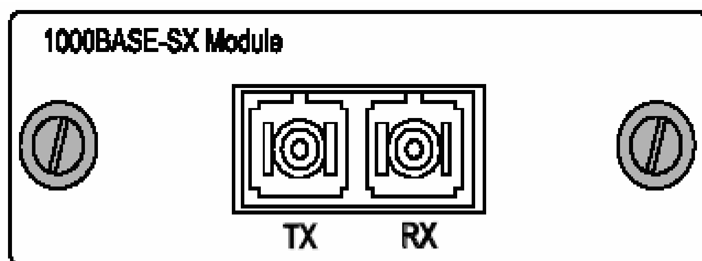


图 1-4 单端口 1000BASE-SX 千兆模块

使用多模光纤电缆，1000BASE-SX 端口能连接 550 米远的远程站点。1000BASE-SX 千兆模块以 1Gbps 的速率操作，它支持全双工模式和流量控制。此模块适合 SC 接头，但你能使用 SC-ST 转换器连接 ST 接头到交换机。

可选的 1000BASE-LX 模块

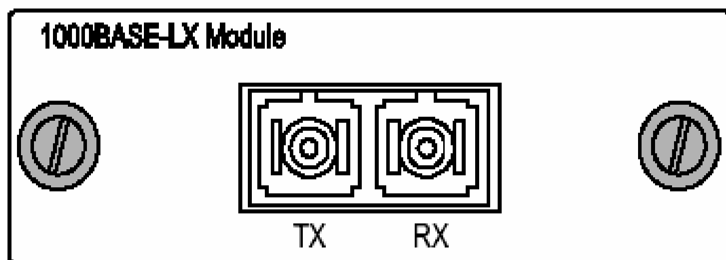


图 1-5 单端口 1000BASE-LX 千兆模块

使用单模光纤电缆，1000BASE-LX 端口能连接 5 千米远的远程站点。1000BASE-LX 千兆模块以 1Gbps 的速率操作，它支持全双工模式和流量控制。

可选的 100BASE-FX 单模模块

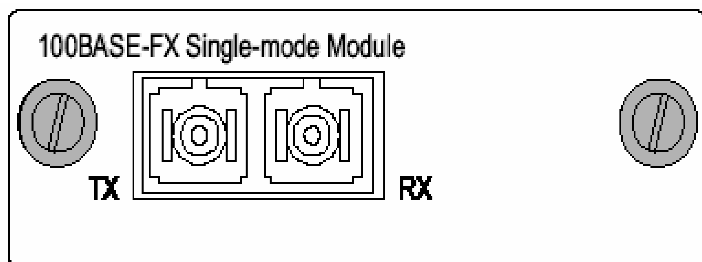


图 1-6 单端口 100BASE-FX 单模模块

使用光纤电缆，100BASE-FX 端口能连接 20 千米远的远程站点。100BASE-FX 千兆模块以固定的 100Mbps 速率全双工模式操作，它支持自适应和流量控制。此模块适合 SC 接头。

可选的 100BASE-FX 多模模块

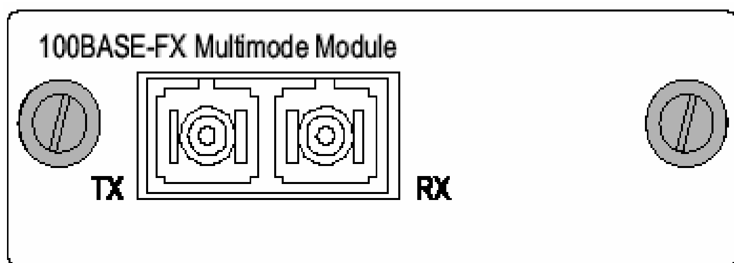


图 1-7 单端口 100BASE-FX 多模模块

使用光纤电缆，100BASE-FX 端口能连接 2 千米远的远程站点。100BASE-FX 千兆模块以固定的 100Mbps 速率全双工模式操作，它支持自适应和流量控制。此模块适合 SC 接头。

电源插口

电源插口位于交换机后面板。标准的电源插口用于插 AC 电源线。

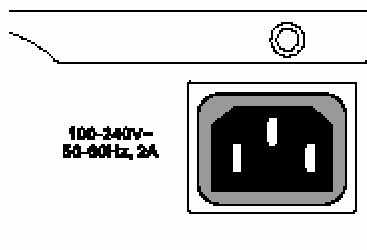


图 1-8 电源插口

特性和优点

连通性

- 24个双速端口用于10或100Mbps以太网连接
- 自适应使每个RJ-45端口能自动选择最适宜的传输模式（半或全双工）
- 独立的RJ-45端口支持自动MDI/MDI-X

- 所有RJ-45端口都支持非屏蔽电缆：对于10Mbps连接选用3、4、5类线，对于100Mbps连接选用5类线
- IEEE 802.3以太网和802.3u快速以太网标准，确保来自不同生产商的集线器、网卡和交换机的兼容性

扩展性

- 可选的一端口1000BASE-SX千兆模块能连接550米远的远程站点，以1Gbps的速率全双工模式操作，支持流量控制自适应。
- 可选的一端口1000BASE-LX千兆模块能连接5千米远的远程站点，以1Gbps的速率全双工模式操作，支持流量控制自适应。
- 可选的一端口1000BASE-T千兆模块能连接100米远的远程站点，以1Gbps的速率全双工模式操作，支持流量控制自适应。
- 可选的一端口100BASE-FX模块能连接2千米或20千米远的远程站点，以100Mbps的速率全双工模式操作，支持流量控制自适应。
- 可选的一端口100BASE-TX千兆模块能连接100米远的站点，以10/100Mbps的速率，全/半双工模式操作，支持速度、双工模式、流量控制自适应。

性能

- 透明桥接
- 聚合带宽达到9.6Gbps
- 8K MAC地址表
- 以线速过滤并转发
- 桌面或机架安装

管理

- LED“时刻”监控容易排除故障
- 管理代理：
- ◆ 支持Telnet，SNMP和基于网络的接口
- ◆ 管理整个交换机in-band或out-of-band
- ◆ 支持多达VLAN 127个组
- ◆ 服务质量支持4个级别的优先级
- ◆ 基于IGMP侦听进行多播交换
- ◆ 端口聚合，支持4组trunk，每组trunk可包含2、4、8个端口

第二章 网络规划

交换简介

交换机允许同时传输多个数据包。这就是说它能比路由器或网桥更有效的分割网络。因此交换机已成为当今网络技术中一个重要的组成部分。

当网络接入点处（如高容量文件服务器的网卡）由拥塞引起瓶颈时，感受到拥塞的设备（服务器或集线器）能直接连接到一个交换端口。此外，

全双工模式使专段的带宽加倍，从而使吞吐量达到最大值。

若网络基于转发器（集线器）技术，则终端站点间的最大距离受到限制。对于以太网，每对站点间可能有多达 4 个集线器；对于快速以太网，有 2 个。这称为跨越记数。但是交换机将跨越记数的值变为零。因此通过交换机将网络再分成更小、更易管理的网段，并将各段结合到更大的网络，从而除去限制。

使用传统的线缆和网卡，在以太网或快速以太网中能容易的配置交换机，可大大增进带宽。

应用举例

交换机能分发因特网访问到多住处或多出租的建筑（MDU/MTU）个人用户，如公寓、商务楼或酒店等。一些特性描述如下。

带宽配置连接

交换机为 MDU/MTU 中的个人用户提供了带宽配置连接。依用户所需，这些连接的带宽能被配置为阈值的 8 个级别。阈值的范围见下表。

端口：10M/100M/1000M （单位：bps）

312K	625K	938K	1.25M	2M	4M	6M	8M
3.12M	6.25M	9.38M	12.5M	20M	40M	60M	80M
31.2M	62.5M	93.8M	125M	200M	400M	600M	800M

注意：在网络可控制台接口中，这些值可以被配置为总端口带宽的3-80%。

专用VLAN

通过配置每个交换机端口到它的专用VLAN（PVLAN），**就能实现对每个用户安全的端口对端口隔离。在这个配置中，交换机只能在每个端口和上连端口（模块端口）间转发数据。**

连通性选项

光纤技术比其他媒质类型允许连接更长的电缆。使用可选的100BASE-FX**模块，多模光纤连接可远达**2**千米，单模光纤连接可远达**20**千米。**

在下图中，两个交换机正对建筑中的个人用户提供带宽配置的连接。安装在第一台交换机中的100BASE-FX**单模模块提供远程上连连接。通过连接到**100BASE-FX**单模上连模块的光纤，第二台交换机被级联。**

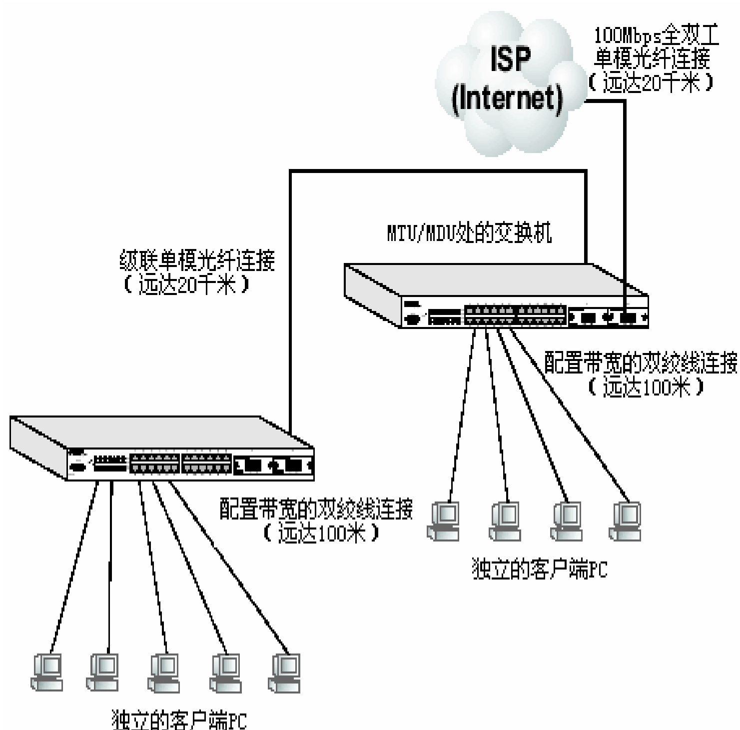


图3-6 带宽配置连接

连接规则

当添加集线器（转发器）到网络时，请遵照下列以太网、快速以太网、千兆以太网的连接规则。但注意：因为交换机将已连设备的路径分为单独的冲突域，所以计算级联长度时，不包括交换机或所连的电缆。

1000 Mbps 千兆以太网冲突域

对于 1000BASE-SX，光纤电缆的最大长度

光纤尺寸	光纤带宽	电缆的最大长度
62.5/125 微米	160 MHz/km	2-220 m (7722 ft)
	200 MHz/km	2-275 m (7902 ft)
50/125 微米	400 MHz/km	2-500 m (71641 ft)
	500 MHz/km	2-550 m (71805 ft)

对于 1000BASE-LX，光纤电缆的最大长度

光纤尺寸	光纤带宽	电缆的最大长度
9/125 微米	N/A	2 米-5 千米

对于 1000BASE-T，光纤电缆的最大长度

类型	接头	电缆的最大长度
5，5E 类 100 欧姆 UTP	RJ-45	100m

100Mbps 快速以太网冲突域

类型	电缆类型	电缆的最大长度
100BASE-TX	5 类 100 欧姆 UTP 或 STP	100 米

100BASE-FX 多模	50/125 或 62.5/125 微米核心多模光纤（MMF）	2 千米
100BASE-FX 单模	9/125 微米核心单模光纤(SMF)	20 千米

II 级转发器的规则

在同一个 100BASE-TX 冲突域中，在任意两个 PC 或其他站点间，可以是：

- 多达 3 个链接段
- 2 个 II 级转发器（集线器）

I 级转发器的规则

在同一个 100BASE-TX 冲突域中，在任意两个 PC 或其他站点间，可以是：

- 多达 2 个链接段
- 1 个 II 级转发器（集线器）

使用转发器最大网络直径

转发器类型和数目	双绞线 100BASE-TX
1 II 级	200 米
1 II 级	200 米
2 II 级	205 米

10 Mbps 以太网冲突域

在同一个 100BASE-TX 冲突域中，在任意两个 PC 或其他站点间，可以是： ● 多达 5 个连续的链接段 ● 多达 4 个转发器（集线器） ● 多达 3 个密集电缆段，即，段连接 2 个或多个 PC（仅限同轴电缆网络）

最大以太网电缆距离

电缆类型	电缆的最大长度
3、4、5 类双绞线	100 米
细同轴电缆	185 米

应用要点

1． 全双工操作仅适用点对点访问（如当交换机连到工作站、服务器或其他交换机时）。当交换机被连接到集线器、那么两个设备必须以半双工模式操作。
2． 连接到集线器的端口避免使用流量控制，除非它需要解决一个问题。否则背压干扰信息可能会降低网段的性能。
3． 多模光纤模块适合 SC 接头，但是你能使用 SC-ST 接头转换器连接 ST 接头到交换机。如果你不使用 ST 接头转换器，请确认你从模块上的 RX（TX）端口到目标设备的 TX（RX）进行接线。
4． 对于单一交换链接，光纤电缆的长度限制如下：
   1000BASE-SX/LX：多模光纤 550 米或单模光纤 5 千米

100BASE-FX：多模光纤 2 千米或单模光纤 20 千米

但是，计算最大电缆长度时，必须考虑电源预算。

第三章 安装交换机

选择安装位置

安装位置——在安装交换机之前，确定它相对于其它设备和装置的位置和方向：

· 在交换机的前面，留出至少7.6 cm 的空间安装双绞线和光缆。

· 在交换机的后面，留出至少3.8 cm 的空间安装电源线。

· 在交换机的四周，留出至少7.6 cm 的空间散热，除非交换机安装在一个敞开式EIA/TIA机架上。

箱内物品

- 本款交换机
- 四个橡胶垫
- 支架安装套件。包含两个安装支架、四个螺丝（用于在机架上安装交换机）
- 电源线
- RS-232 控制台电缆
- 用户手册
- 质保卡（请填好寄回我公司）

安装

交换机能安装在标准的 19 英寸机架或桌面上。每处的安装说明如下。

安装可选的模块：在安装交换机之前，请确认安装可选的模块，如果你

已经购买滑入1000BASE-T，1000BASE-SX，1000BASE-LX，100BASE-FX，1000BASE-X GBIC 或联合1000BASE-T/SFP媒质扩展模块，请即刻安装这些模块，按照本章的“安装可选的模块”中的指示。

将交换机安装在机架上

在安装交换机前，注意下列事项：

温度：由于温度机架中的温度高于室内环境的温度，请核查机架环境温度在规定的范围之内（见附录 C）。

机械负载：请勿将任何装置放于安装在机架上的交换机上。

电路过载：请确认供电回路没有过载。

接地：安装在机架上的设备应该正确接地。

安装设备

1． 使用包装中提供的螺丝将支架安装在设备上。

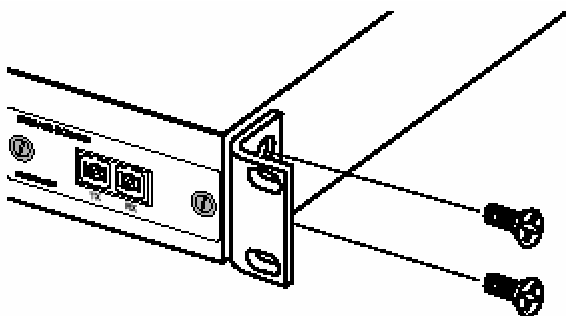


图 3-1 安装支架

2． 使用 4 个螺丝（自备）将交换机安装到机架上。

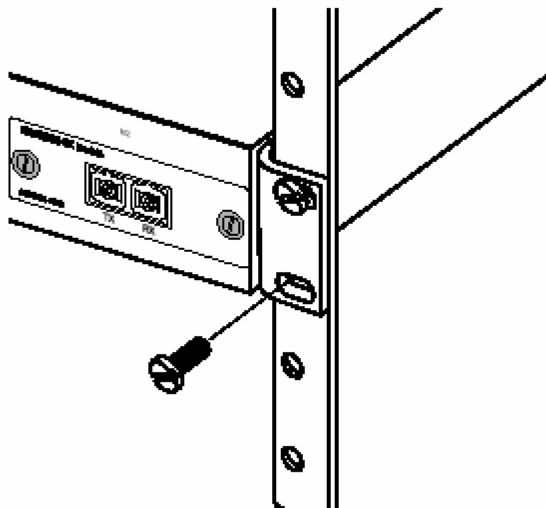


图 3-2 将交换机安装到机架上

3． 如果只安装一台交换机，请跳至本章尾处的“连接电源”。

4． 如果安装多台交换机，请依次安装在机架上。

将交换机安装在桌面上

1． 将自粘塑胶脚垫 (随包装附带)粘到第一台交换机底部的 4 个凹入处。

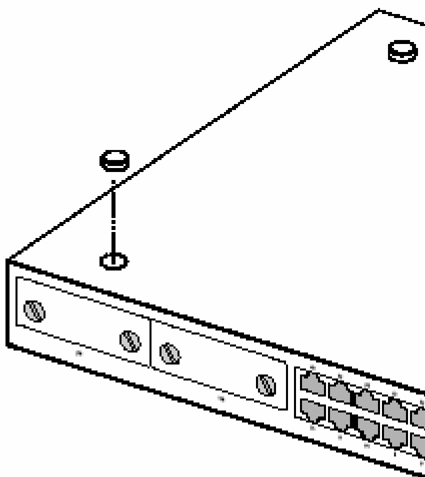


图 3-3 安装脚垫

2． **请置于平面上，靠近** AC **电源并确保交换机四周通风干燥。**

3． **如果只安装一台交换机，请跳至本章尾处的"连接电源"。**

4． **如安装多台交换机，将每台交换机的脚垫一一粘好。整齐堆叠。**

安装可选的模块

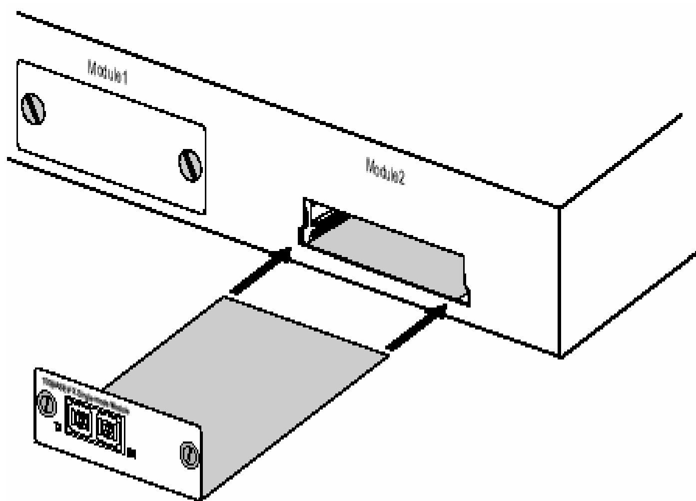


图 3-4 安装可选的模块

警告：当交换机通电时，请勿安装滑入模块。安装时，请关闭交换机电源。

1． **关闭交换机电源 (模块不支持热插拔)。**

2． **用平头螺丝刀旋开两颗固定螺丝，取下右下槽位上的面板。**

3． **打开模块包装前，将包装袋与交换机壳接触一下以放掉静电。**

4． **从防静电包装袋中取出模块。**

5． **沿导轨将模块水平轻轻推入插槽，确保与插座可靠连接。**

6． **确定模块与插座正确连接后，旋紧固定螺丝。**

连接电源

1． **将电源线插入交换机后面板的电源插孔。**

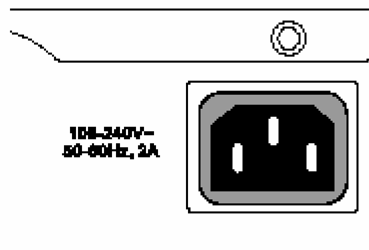


图 3-5 电源插孔

2． **将电源线的另一端插入** 3 **脚电源插座。**

3． **检查前面板的** LED **指示灯已亮。如果不亮，检查电源线是否正确插入。**

第四章 网络连接

连接网络设备

交换机可以连接到PC中的10或100Mbps网卡，服务器，以太网和快速以太网集线器和交换机。使用可选的100BASE-FX模块它也可以连接到远程设备。

双绞线设备

每台设备需要一个屏蔽或非屏蔽双绞线（STP 或 UTP），两端均有 RJ-45 端口。对于 100BASE-TX 连接，使用 5 类线；对于 10BASE-T 连接，使用 3，4，5 类线。

电缆的概念

两端口间的双绞线连接必须有传输和接收线缆的交叉才能运做。此交叉能在两端口中的任何一个或连接端口的线缆中被执行。

PC 中的网卡端口和服务器不包含内部的配线交叉，它们被称为直通（MDI）端口。因此，大多数交换机和集线器端口执行一个内置的交叉——称为固定交叉（MDI-X）端口——因此使用标准的直通线它们能被连接到 PC 或服务器。一些交换机和集线器也有 MDI 端口，因此使用直通线它们能连接另一个交换机/集线器的 MDI-X 端口。若要在两个只有固定 MDI-X 端口的交换机/集线器中进行连接，配线交叉则必须在线缆中执行——称为交叉线。

交换机上的 RJ-45 端口支持自动 MDI/MDI-X 操作，这就是说它们自动侦察链路中的接线，并配置为 MDI 或 MDI-X。因此对于这些端口，你能使用标准的直通双绞线来连接其他网络设备（PC、服务器、交换机、集线器或路由器）。注意必须对自动 MDI/MDI-X 操作激活自适应确保其正确运做。

连接到 PC、服务器、交换机、集线器和交换机

警告：不要把电话插头插入任何一个 RJ-45 端口。这会损坏交换机。请使用符合 FCC 标准的有 RJ-45 的双绞线。

1． 将双绞线一端插入设备的 RJ-45 插孔。

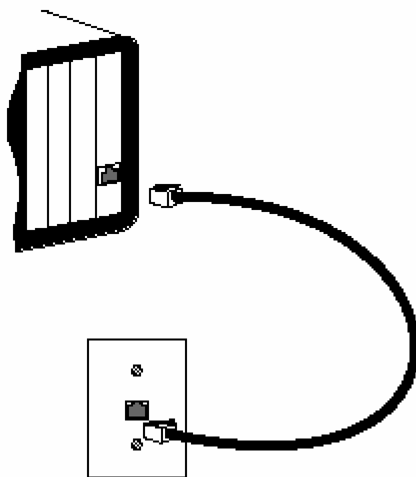


图 4-1 进行双绞线连接

2． 如果设备是 PC 卡、交换机在配线柜中，请将线缆的另一端插入连有配线盒的墙壁插孔。（参看下一

页“配线柜的连接”)。否则，将另一端插入交换机的可用端口。

3. 请确认每股双绞线长度不超过 100 米。

注意：当连接到共享的冲突域（如有多工作站的集线器)。交换机端口必须设置为半双工模式。

4. 每个连接完成后，对应每个端口的绿色 Link LED（交换机上）将发亮，显示连接有效。

配线柜的连接

今天，卡口已经成为许多新款机架的一部分。实际上它是配线板的一部分。配线柜中的连接指示如下。

1. 将接插线的一端插入交换机上的可用端口，另一端插入配线板。
2. 如果没有准备好，将线缆的一端插入配线板的背部（背部有卡口)，另一端插入墙上的插孔。
3. 将线缆贴上标签，以便以后解决故障。

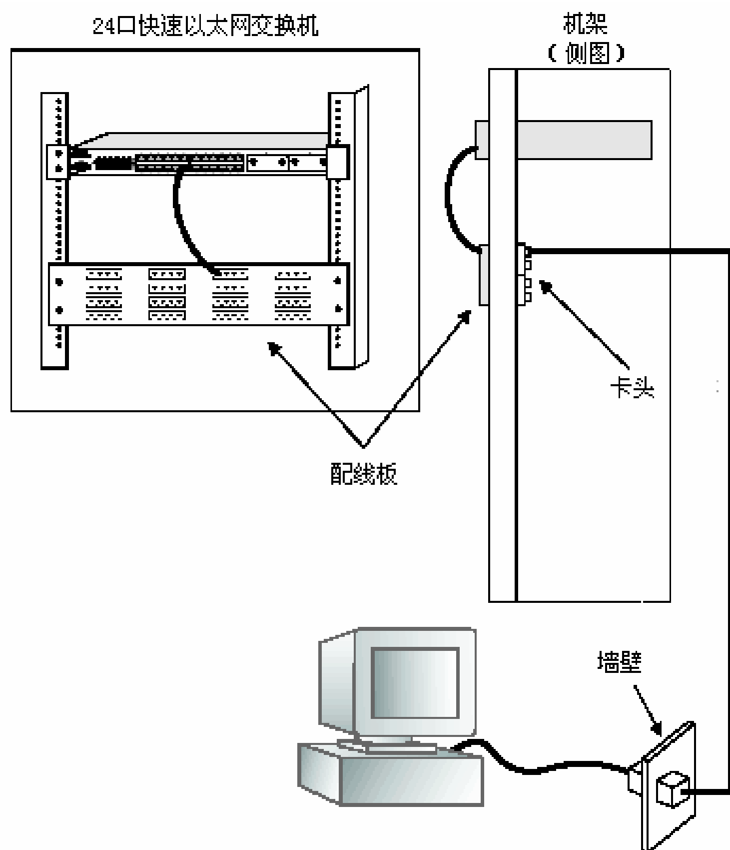


图 4-2 配线柜的连接

光纤设备

一个可选的滑入 100BASE-FX **模块可用于长距离连接。**1000BASE-X **模块也能用于交换机间的骨干连接，或用于连接到高速服务器。**

每个多模光纤端口需要 50/125 **或** 62.5/125 **微米多模光纤电缆，两端均有** SC **接头。如果你需要用** 62.5/125 **微米电缆（有** ST **型接头）连接到一个设备，请使用** SC-ST **转换器。**

每个单模光纤端口需要 9/125 **微米单模光纤电缆，两端均有** SC **接头。**

警告：此交换机使用激光在光纤电缆上传输信号。激光符合 1 **级激光产品的要求，常规操作对眼睛无害。但是通电时，请勿直视传输端口。**

1． **除去并保留** SC **端口的橡皮套。不使用时，套上橡皮套以保护光纤。**
2． **检查光纤终结器是否干净。将干净的纸巾或棉球稍稍蘸湿，轻轻擦拭电缆插头。弄脏的光纤终结器会降低光传输的质量，使端口性能受到影响。**
3． **将电缆的另一端连接到交换机的** SC **端口，另一端连到另一台设备的** SC **端口。由于** SC **接头有编号，电缆只能从一个方向插入。**

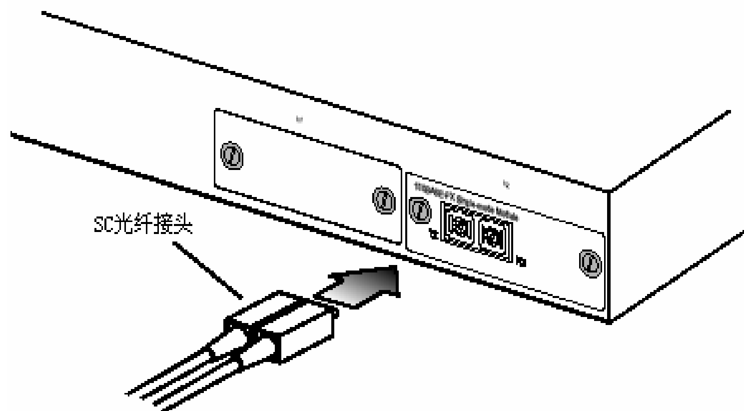


图 4-3 SC 端口的连接

4． **连接完成后，请检验交换机前面板上相应模块的**Activity LED**已亮，说明连接有效。**

注意：如果你使用SC-ST**转换器，请确认连接转换器的**TX（RX）**端口到另一台设备的**RX（TX）**端口。**

附录 A 疑难解答

通过指示灯诊断

疑难解答表	
故障	**采取措施**
Power LED不亮	● 内部供电失败或未接通 ● 检查交换机、电源线、墙壁电源插座间的连接 ● 如果交换机安装在机架上，请检查接线板的连接 ● 请联系我公司技术支持部
Link LED不亮	● 确认交换机和所连的设备通电 ● 确认接线插入交换机和相应的设备 ● 确认使用正确的电源类型，长度不超限 ● 检查所连设备的适配器和接线是否正常，如有必要请更换之

电源及冷却系统故障

如果插入电源线后指示灯不亮，电源插座、电源线或内部电源模块可能有问题，但是如果机器运行一段时间后自动关机，则需要检查电源插头是否松动、是否停电、供电电压是否波动、检查机箱右侧风扇是否运转正常。如果仍然不能发现故障，则内部电源模块可能出现故障。请联系我公司寻求帮助。

安装

确认所有系统部件均已正确安装，如果某个或多个部件出现故障(如电源线或网线)，换到另一个所有其它部件均正常的环境中测试其是否正常。

In-Band 访问

使用 Telnet**、网络浏览器或其他网络管理软件，你能访问交换机的管理代理。但是你必须先对交换机配置有效的** IP **地址，子网掩码和默认网关。如果你无法连接到管理代理，请检查你是否有有效的网络连接。然后检查你是否输入正确的** IP **地址。并确认端口已经激活。如果已经激活的，请检查连接交换机和远程站点的网线。**

注意：你能配置管理代理接受 1-4 **个同时发生的远程登录会话。如果最大的会话数已经存在，那么一个额外的** Telnet **连接将不能登录系统。**

附录 B 线缆

规格

线缆类型及规格			
线缆	类型	最大长度	接头
10BASE-T	3,4,5 类-100 欧姆 UTP	100 米（328 英尺）	RJ-45
100BASE-TX	5 类-100 欧姆 UTP	100 米（328 英尺）	RJ-45
100BASE-FX	50/125 或 62.5/125 微米核	2 公里（1.24 英里）	SC
100BASE-FX	9/125 微米核心单模光纤电缆	20 公里（12.43 英里）	SC
1000BASE-SX	50/125 或 62.5/125 微米核	见下表	SC
1000BASE-LX	9/125 微米 SMF	5 公里	SC
1000BASE-T	5 类线，5E100 欧姆 UTP	100 米	RJ-45

1000BASE-SX 光纤规格		
光纤直径	光纤带宽	最大线缆长度
62.5/125 微米 MMF	160 MHz/km	2-220 米

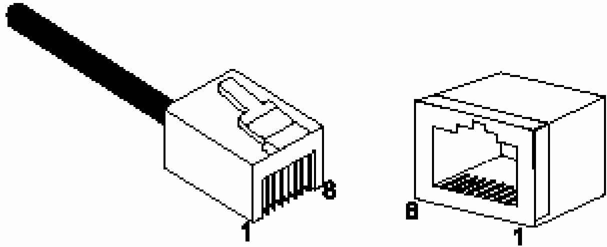
	200 MHz/km	2-275 米
50/125 微米 MMF	400 MHz/km	2-500 米
	500 MHz/km	2-550 米

双绞线和管脚分配

警告:不要把电话插头插入任何一个 RJ-45 端口。只用符合 FCC 标准的双绞线，两端均有 RJ-45 接头。

对于 100BASE-TX/10BASE-T 连接，双绞线必须有两对线。每一对用两种不同的颜色来区分。例：一股红色，另一股红白条纹相间。线缆两端必须有 RJ-45 接头。

下图说明了 RJ-45 接头如何编号，请确认插入时方向一致。



10BASE-T/100BASE-TX 管脚分配

RJ-45 连接采用非屏蔽双绞线(UTP)或屏蔽双绞线(STP)：10Mbps 连接采用 100 欧姆 3，4，5 类线，100Mbps 采用 100 欧姆 5 类线。此外，切记任何双绞线连接长度不得超过 100 米。

RJ-45 端口支持自动 MDI/MDI-X 操作，你可以使用直通线连接 PC 或服务器，或连接其他交换机或集线器。100BASE-TX 模块上的 RJ-45 端口是

一个 MDI-X 端口，你能使用直通线连接到 PC 或服务器。在直通线中，管脚 1、2、3、6 在线缆的一端，分别连通线缆另一端的管脚 1、2、3、6。对于连接到有 MDI-X 端口的交换机或集线器，则必须使用交叉线。

管脚	MDI-X 信号名	MDI 信号名
1	接收数据＋（RD+）	输出数据＋（TD+）
2	接收数据－（RD-）	输出数据－（TD-）
3	输出数据＋（TD+）	接收数据＋（RD+）
6	输出数据－（TD-）	接收数据－（RD-）
4，5，7，8	未用	未用

注意：“+”“-”代表线缆极性。

直通线

如果双绞线加入两个端口且只有其中一个端口有内部交叉（MDI-X），那么这两对线必须是直通线。

直通线 RJ-45 管脚分配	
终端 1	终端 2
1（RD+）	1（TD+）
2（RD-）	2（TD-）
3（TD+）	3（RD+）

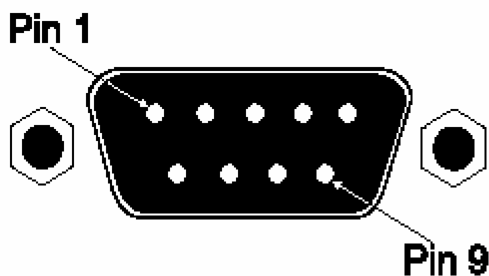
6（TD-)	6（RD-)

交叉线

如果双绞线加入两个端口且两个端口都标注“ X ”(MDI-X)，或两个端口都没有标注“ X ”(MDI），那么接线时必须使用交叉线。

交叉 RJ-45 管脚分配	
终端 1	**终端** 2
1（TD+)	3（RD+)
2（TD-)	6（RD-)
3（RD+)	1（TD+)
6（RD-)	2（TD-)

控制台管脚分配



DB-9 端口管脚分配

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #	PC DB25 DTE Pin #
BB	104	**RxD** (Received Data)	2	2	3
BA	103	**TxD** (Transmitted Data)	3	3	2
AB	102	**SG** (Signal Ground)	5	5	7

其他管脚未使用。

Console Port to 9-Pin DTE Port on PC

Switch's 9-Pin Serial Port	Null Modem	PC's 9-Pin DTE Port
2 RXD	<--------- TXD ------------	3 TXD
3 TXD	----------- RXD ---------->	2 RXD
5 SGND	----------- SGND ----------	5 SGND

其他管脚未使用。

Console to 25-Pin DTE Port on PC

Switch's 9-Pin Serial Port	Null Modem	PC's 25-Pin DTE Port
2 RXD	<--------- TXD ------------	2 TXD
3 TXD	----------- RXD ---------->	3 RXD
5 SGND	----------- SGND ----------	7 SGND

其他管脚未使用。

附录 C 规格

物理特性

基本单元

端口

24 10BASE-T/100BASE-TX，**自适应**

2**个插槽，可选的**100BASE-FX, 1000BASE-T, 100BASESX,**或**
1000BASE-LX**模块**

网络接口

10BASE-T： RJ-45 (100-ohm, UTP**线缆**; 3, 4, 5**类**)

100BASE-TX：RJ-45 (100-ohm, UTP**线缆**; 5**类**)

端口1-24： RJ-45 **接头，自动**MDI/MDI-X

传输速率

10**和**100 Mbps

传输模式

全或半双工

缓冲机构

每系统 6 Mbyte

总带宽

9.6 Gbps

交换数据库

8K MAC**地址**

LEDs

系统：Power

端口：Link, Speed

重量

3 kg (6 lb 10 oz)

尺寸

44 x 23 x 4.3 cm (17.32 x 9.05x 1.69 in.)

温度

操作：0 - 50 °C (32 - 122 °F)

存储：-40 - 70 °C (-40 - 158 °F)

湿度

操作：10% - 90%

电源

内部，变压器：100 -240 VAC, 50 - 60 Hz

电耗

60 W **最大**

散热

205 BTU/hr **最大**

最大电流

3.0 A @ 115 VAC, 2.0 A @ 240 VAC

管理特性

In-Band 管理

Telnet**，基于网络的**HTTP**，或**SNMP**管理器**

Out-of-Band 管理

RS-232 DB-9 **控制台口**

软件负载

TFTP 或 Web (HTTP) in-band，或XModem out-of-band

MIB 支持

MIB II (RFC1213)，Bridge MIB (RFC 1493, 无静态表)

标准

IEEE 802.3 以太网， IEEE 802.3u快速以太网

IEEE 802.1p priority tags

IEEE 802.3ac VLAN tagging

IEEE 802.1Q VLAN网桥管理

IEEE 802.3x 全双工流量控制

ISO/IEC 8802-3

SNMP (RFC 1157), ARP (RFC 826), MIB II (RFC 1213), Bridge MIB (RFC 1493)

遵从

CE Mark

散发

FCC Class A

Industry Canada Class A

EN55022 (CISPR 22) Class A

EN 61000-3-2/3

VCCI Class A

C-Tick - AS/NZS 3548 (1995) Class A

免疫

EN 61000-4-2/3/4/5/6/8/11

安全

CSA/NRTL (CSA 22.2.950 & UL 1950)

IEC 60950

第二部分

BitStream3224TM+

管理手册

第一章 初始配置

连接交换机

配置选项

本款交换机包含有内置的网络管理代理，该代理提供了大量的管理选项，其中包括 SNMP,RMON 和基于 Web 的接口。PC 机可以通过命令行界面(CLI)直接连到交换机上,对它进行配置和监控。

注意：默认情况下,交换机的 IP 地址未分配。如果要修改 IP 地址，请参阅本章“设置 IP 地址”。

因为交换机里有 HTTP Web 代理,你可以通过标准网页浏览器(如 Netscape Navigator 6.2 以上版本和微软的 IE 5.0 以上版本)来配置交换机参数，监控端口连接和以图的形式显示状态参数等。任何一台连接到网络上的计算机都可以访问交换机的 Web 管理界面。

本交换机的管理模块是基于SNMP（简单网络管理协议）的,它允许任何一个网络上的系统通过管理软件对交换机进行管理,比如本公司的免费软件:AccView或HP OpenView。

直接连接到交换机上的 RS-232 串行控制端口,或者通过网络 Telnet 连接远程登录,都可以访问 CLI 程序。

交换机的 CLI 配置程序,Web 接口和 SNMP 模块提供了以下的管理功能:

- 设置不多于 16 个的用户名及其密码
- 给每一个 VLAN 设置一个 IP 接口
- 配置 SNMP 参数
- 激活/禁用任意端口
- 设置端口的速率/双工模式
- 通过速率限制配置端口带宽
- 给端口隔离分配独立的 VLAN
- 配置不超过 127 个的 IEEE802.1Q VLAN
- 激活 GVRP,自动进行 VLAN 注册
- 配置 IGMP 组播过滤
- 系统固件的 TFTP 上传和下载
- 交换机配置文件的 TFTP 上传和下载
- 配置生成树参数
- 配置服务类别(CoS)优先队列
- 配置多达 4 个静态 trunk
- 激活端口镜像
- 在任何端口上设置广播风暴控制
- 显示系统信息和参数

需要的连接

把交换机的 RS232 串行口连接到 PC 或终端上,可以对交换机进行监控和配置。交换机附带一根串口线。

要把交换机连接到 VT-100 兼容的终端或运行终端仿真软件的 PC 上,可以使用箱内附带的串口线,也可以使用其它类似的兼容的线，见附录 B。

把终端连接到控制口上,需完成以下步骤:

1. 把控制线接到终端或PC的串行口上,并把DB-9连接器上的螺丝拧紧。
2. 把线的另一端接到交换机的RS232串行口上。
3. 检查并确认终端的仿真软件按以下值设置:
    - 选择相对应的串口(COM 端口1或COM 端口2)
    - 把速率设为9600 baud
    - 把数据格式设为8个数据位,1个停止位,无奇偶
    - 把流量控制设为无
    - 把仿真模式设为VT100
    - 当使用的是超级终端,选择Terminal键,而不是Windows键

注意:

1. 当使用微软Windows 2000里的超级终端,必须安装Windows 2000的Service Packet 2或更新版本。请访问www.Microsoft.com 以了解和Windows 2000 Service Packet 2有关的信息。
2. 请参阅第三章"行命令"获取控制口配置选项的详细信息。
3. 一旦正确安装了终端,控制台登录界面将显示。

如果需要了解如何使用 CLI,请参阅第三章首页"使用命令行界面"。如需CLI命令的详细列表和使用CLI的详细信息,请参阅第三章"命令集"。

远程连接

在通过网络连接访问交换机内建的代理前,首先必须使用控制口连接、DHCP 或 BOOTP 协议先给交换机配置一个有效的 IP 地址,子网掩码和默认网关。

默认的 IP 地址未分配。如需手动配置 IP 地址或激活 DHCP 或 BOOTP 动态分配,请参阅本章“设置 IP 地址”。

注意：这款交换机同时支持 4 个并发的 Telnet 会话。

配置完交换机的 IP 参数后,可以在网络的任何一个地方访问它的配置程序。任何一台网络上的计算机都可以使用 Telnet 访问交换机的内建的配置程序。同时也可以使用 Web 浏览器或者网络管理软件对交换机进行管理。

注意：内建的程序仅仅提供对基本配置功能的访问。为了访问所有范围的 SNMP 管理功能，你必须使用基于 SNMP 的网络管理软件。

基本配置

连接控制口

CLI 程序提供了两个不同的命令级别---普通访问(Normal Exec)和特权访问(Privileged Exec)。 普通访问所包含的命令行仅仅是特权访问一个有限的子集,且只允许显示信息和使用基本的功能。为了充分地配置交换机的参数,必须以特权身份来访问 CLI。

两种 CLI 级别的访问都由用户名和密码控制。交换机给每个级别的访问都设有一个默认的用户名和密码。使用默认用户名和密码以特权身份登录 CLI,请执行以下步骤:

1. 启动控制口连接,按<Enter>。“用户访问身份确认”程序启动。
2. 用户名提示,输入“admin”。

3. 密码提示,默认密码为空。
4. 会话开始,CLI 显示“Switch#”,也即意味着你已成功以特权访问身份访问。

设置密码

注意:如果你是第一次登录 CLI 程序,建议使用“username”给默认用户名定义新的密码,把它们记录下来并保存在安全的地方。

密码最多由 8 个区分大小写的阿拉伯数字或字符组成。为了防止未授权访问交换机,设置密码如下:

1. 打开控制台窗口,以默认的用户名和密码“admin”登录:
2. 输入“configure”,按回车键。
3. 输入“username guest pasword 0 *password*”为普通访问设置用户名和密码,其中的 *password* 即是你的新密码,按回车键。
4. 输入“username admin password 0 *password*”,为特权访问设置用户名和密码,其中的 *password* 就是你的新密码。按回车键。

```
User Access Verification

Username: admin
Password:

      CLI session with the BitStream BS3224TM+ is opened.
      To end the CLI session, enter [Exit].

Switch#configure
Switch(config)#username guest password 0 password
Switch(config)#username admin password 0 password
Switch(config)#
```

设置 IP 地址

为了能从网络上对交换机进行管理,必须给它建立 IP 地址信息。可以通过以下两种方式实现。
手动——必须手动输入信息,包括 IP 地址和子网掩码,如果管理工作站和交换机不在同一个 IP 子网,必须给出默认网关路由器。

动态——交换机发送 IP 配置请求给 BOOTP 或 DHCP 服务器。
注意：只有一个 VLAN 接口可以分配到一个 IP 地址(默认是 VLAN 1)。这定义了管理者 VLAN,通过这个 VLAN 可以获得对交换机的管理访问。如果分配了一个 IP 地址给其它的 VLAN,新的 IP 地址覆盖了旧的 IP 地址并成为新的管理 VLAN。

手动配置

可以手动分配一个 IP 地址,如果交换机和管理工作站在不同的网段上,必须指定一个默认的网关。有效 IP 地址由四个 0-255 的十进制数字组成,由点号分开。不符合这种格式的将不被 CLI 程序接受。
注意：默认情况下，交换机 IP 地址未分配的。

在可以给交换机分配一个 IP 地址前,必须从网络管理员处得到以下信息:

- 交换机的 IP 地址。
- 网络的默认网关。
- 网络的掩码。

给交换机分配 IP 地址,完成以下步骤:

1. 在 Privileged Exec 全局配置模式提示下:输入“interface

vlan 1”以存取接口配置模式,按回车键。

2. 输入“ip address ip-address netmask”,其中 IP-address 就是交换机的 IP 地址,netmask 是网络的掩码。按回车键。
3. 输入“exit”退出,按回车键。
4. 设置交换机所在的网络的默认网关的 IP 地址。输入“ip default-gateway gateway”,其中的 gateway 就是网关的 IP 地址。按回车键。

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.5 255.255.255.0
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.254
Switch(config)#
```

动态配置

如果选择“bootp”或“dhcp”选项,IP 将被激活但不会起作用直到收到 BOOTP 或 DHCP 的应答。因此必须使用“ip dhcp restart”命令启动广播服务请求。请求将被周期性地发送以获得 IP 配置信息。(其中包括 IP 地址,子网掩码和默认网关)

如果“bootp”或“dhcp”被保存在启动-配置文件里,一旦交换机开机,它就发送广播服务请求。

配置交换机自动的和网络上的 BOOTP 或 DHCP 地址分配服务器通信,请完成以下步骤:

1. 在 Privileged Exec 全局配置提示下,输入“interface vlan 1”以存取接口配置模式,按回车键。
2. 在接口配置模式下,使用以下命令中的一个:

   ·从 DHCP 获取 IP 设置,输入“ip address dhcp”,回车。

·从 BOOTP 获取 IP 设置,输入“ip address bootp”,回车。

3. 输入“exit”退出,回车。
4. 输入“ip dhcp restart”以开始广播服务请求,回车。
5. 等几分钟,检查 IP 配置设置,输入“show ip interface”,回车。
6. 输入“copy running-config startup-config”以保存配置改变。输入启动文件名,回车。

```
Switch(config)#interface vlan 1
Switch(config-if)#ip add dhcp
Switch(config-if)#end
Switch#ip dhcp restart
Switch#show ip interface
 IP address and netmask: 0.0.0.0 255.0.0.0 on VLAN 1,
 and address mode: DHCP.
Switch#
```

激活 SNMP 管理访问

这款交换机能配置成能够接收来自SNMP应用(如AccView或HP OpenView)的命令。可以把交换机配置成(1)应答SNMP请求,或(2)生成SNMP陷阱。

当 SNMP 管理工作站发送请求给交换机(无论是返回信息还是设置参数),交换机将提供所要求的数据或设置指定的参数。交换机同时也能被配置通过陷入信息发送信息给 SNMP 管理者,以通知管理者发生了特定的事件。

团体字符串

团体字符串用来控制对 SNMP 工作站的管理访问,即授权 SNMP 工作站从交换机接收陷入信息。因此必须给特定的用户或用户群分配团体字符串,同时设置访问级别。

默认字符串是:

・public ——只读访问,授权的管理工作站只能接收 MIB 对象。

・private ——读写访问。授权的管理工作站既能接收也能修改 MIB 对象。

注意:如果你不打算使用 SNMP,建议删除这两个默任团体字符串。如果没有团体字符串,到交换机的 SNMP 管理访问被禁用。

为了防止未授权访问,建议修改默认团体字符串。

配置团体字符串,请完成以下步骤:

1. 在 Privileged Exec 全局配置模式提示下,输入“snmp-server community string mode”,其中 string 就是团体字符串,mode 是 re(读/写)或 ro(只读)。回车。
2. 删除团体字符串,输入“no snmp-server community string”,其中 string 就是要删除的团体字符串。回车。

```
Switch(config)#snmp-server community abc rw
Switch(config)#snmp-server community private
Switch(config)#
```

陷阱接收器

可以指定接收来自交换机的陷阱的 SNMP 工作站。

配置一个陷阱接收器,请完成以下步骤:

1. 在 Privileged Exec 全局配置模式提示下,输入“snmp-server host host-address community-string”,其中 host-address 就是陷入接收器的 IP 地址,community-string 是关联的字符串。回车。
2. 为了配置交换机发送 SNMP 通知信息,必须至少输入一个 snmp-server

陷入激活命令。输入“ snmp-server enable traps type ”,其中“ type ”或者是 authentication ,或者是 link-up-down。回车。

```
Switch(config)#snmp-server enable traps link-up-down
Switch(config)#
```

保存配置设置

配置命令仅仅修改运行时的配置,当重新启动时并未保存设置。为了保存配置修改,必须使用“ copy ”命令把运行配置拷贝到启动配置文件中去。

要保存现有的配置设置,请完成以下步骤:

1. 在 Privileged Exec 全局配置模式提示下,输入“ copy running-config startup-config ”,回车。
2. 输入启动文件的文件名。回车。

```
Switch#copy running-config startup-config
Startup configuration file name [test]: startup
Write to FLASH Programming.
Write to FLASH finish.
Success.

Switch#
```

管理系统文件

交换机的闪存支持 3 种能被 CLI 程序 、Web 接口和 SNMP 管理的系统文件。交换机的文件系统允许文件被上传 、下载 、拷贝 、删除和设置成启动文件。

这三种类型文件是:

- **配置---这些文件保存系统配置信息且当配置设置被保存是创建。保存配置文件能被选择为系统启动文件或通过 TFTP 上传到服务器去备份。一个名为“Factory_Default_Config。cfg”的文件包含了所有的系统默认设置,该文件不能被删除。**
- **操作代码---启动后被执行的系统代码,即所说的工作代码。这些代码完成交换机的操作并且提供 CLI 、Web 和 SNMP 管理接口。**
- **诊断代码---系统启动时运行的软件,即所说的 POST。这些代码同时提供了这样一种机制:直接通过控制台端口下载固件文件。**

由于闪存容量的限制,交换机只支持一个操作代码文件,两个诊断代码文件。但是只要闪存能装得下,就可以存放尽可能多的配置文件。

在系统闪存里,每种类型的一个文件必须设置成启动文件。在系统启动时,诊断和操作代码文件被设成启动文件开始运行,然后启动配置文件被载入。当系统运行(无须重启系统)时,配置文件也能被载入。

系统默认值

交换机的系统默认值有配置文件“Factory_Default_Config.cfg”提供.为了重设交换机的默认值,该文件应被设成启动配置文件。(见第二章)

下表列出了一些基本系统默认值.

功能	参数	默认值
IP 设置	管理 VLAN	1
	DHCP	激活
	BOOTP	禁用
	用户指定	禁用

	IP 地址	0.0.0.0
	子网掩码	255.0.0.0
	默认网关	0.0.0.0
Web 管理	Http 服务器	激活
	HTTP 端口号	80
SNMP	团体字符串	“public”(只读) “private”(读/写)
	陷阱	认证陷阱：激活 Link-up-down 事件：陷阱
安全	特权 Exec 级别	用户名“admin” 密码 为空
	普通 Exec 级别	用户名 “guest” 密码 “guest”
	从普通 Exec 级别激活特权 Exec	密码 “super”
	RADIUS 认证	禁用
控制台口的连接	波特率	9600
	数据位	8
	停止位	1
	奇偶	无
	本地控制台超时	0(禁用)
端口状态	管理状态	激活
	自适应	激活
	流量控制	禁用

	10/100Mbps 端口性能	10 Mbps 半双工 10 Mbps 全双工 100 Mbps 半双工 100 Mbps 全双工 禁用全双工流量控制
	10/100/1000Mbps 端口性能	10 Mbps 半双工 10 Mbps 全双工 100 Mbps 半双工 100 Mbps 全双工 1000 Mbps 全双工 禁用均衡流量控制
链路聚合	静态 Trunk	无
生成树协议	状态	激活 (默认：所有参数基于 IEEE 802.1D)
	快速转发	禁用
地址表	老化时间	300 秒
虚拟 LANs	默认 VLAN	1
	PVID	1
	可接受的帧类型	全部
	入口过滤	禁用
	GVRP（全局）	禁用
	GVRP（端口接口）	禁用
服务类别	输入端口优先级	0

	循环	Class 0: 1 Class 1: 3 Class 2: 12 Class 3: 48
广播风暴保护	状态	激活(所有端口)
	广播限制速率	缓冲空间的 6%

第二章 配置交换机

使用 Web 界面

本章基于本款交换机的 Web 界面。

交换机提供内嵌的 HTTP Web 代理。使用 Web 浏览器你能配置交换机并观察状态，监控网络活动。Web 代理通过标准的 Web 浏览器（Internet Explore 5.0 以上版本或 Netscape Navigator 6.1 以上版本）能被任何网络中的交换机访问。

你也能使用命令行界面（CLI），通过 Telnet 或连续的控制台口的连接，管理交换机。如要获取更多有关 CLI 使用的信息，参看第三章"命令行界面"。

从 Web 浏览器优先访问交换机之前，首先执行如下操作：

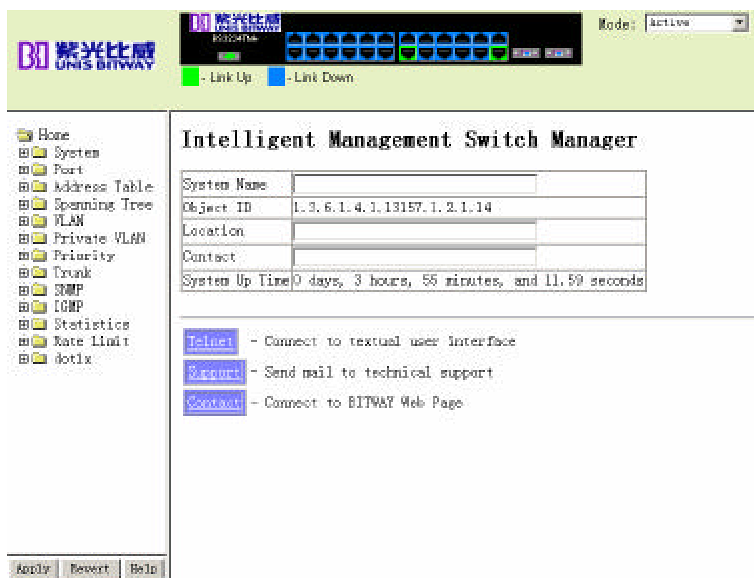
1． 使用带外的串口连接，BOOTP 或 DHCP 协议（参看本章"设置 IP 地址"），用有效的 IP 地址、子网掩码、和默认网关配置交换机。
2． 使用带外的串口连接设置用户名和密码。对 Web 代理访问受到配置程序中相同用户名和密码的控制。（参看本章"配置登录密码"）
3． 输入用户名和密码后，就可访问系统配置程序。

操作 Web 浏览器界面

要访问此界面，首先需输入你的用户名和密码。管理者对所有的配置参数和统计表有读/写访问的权利。默认用户名是"admin"，密码为空。

主页

当 Web 浏览器与交换机 Web 代理连接时，主页显示如下。主页界面左边显示主菜单，右边显示系统信息。主菜单连接用于操作其它菜单，并显示配置参数和统计表。



配置选项

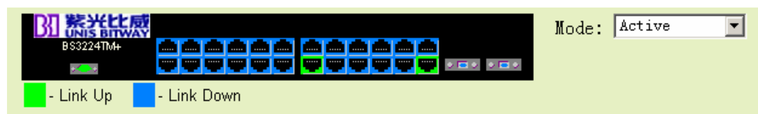
配置参数有一个对话框和下拉列。一旦更改配置，确认点击 " Apply " 或 " Apply Changes " 来确定新设置。下表概述了 Web 页面的配置按钮。

按钮	活动

Apply	对系统设置指定的值
Apply Changes	对系统设置指定的值
Revert	按"Apply"和"Apply Changes"前，取消指定的值和恢复当前的值
Refresh	更新当前页的值

面板显示

Web 代理显示交换机端口的图象，指示每个连接连上或断开。点击端口图象打开端口配置页面。



主菜单

使用 Web 代理，你可以定义系统参数，管理并控制交换机所有端口，或监控网络状态。

基本配置

显示系统信息

通过提供描述名、位置和联系信息，你能容易地识别系统。

命令属性

- **System Name** ——分配给交换机系统的名
- **Object ID** ——交换机的网络管理子系统的 MIB II 目标 ID
- **Location** ——指定系统位置

- **Contact ——系统的管理者响应**
- **System Up Time ——管理代理所用的时间长度**
- **MAC Address[1] ——交换机的物理层地址**
- **Web server[2] ——显示管理访问通过** HTTP **激活或禁用**
- **Web server port[2] ——显示** WEB **接口使用的** TCP **端口数目**
- **POST result[2] ——显示通电后的自检结果**

1． WEB：**参看第三章"设置** IP **地址"**

2． **仅** CLI。

Web ——点击 System, System Information。**对系统管理者指定系统名、位置和联系信息，点击**Apply。（**本页面包含**Telnet**按钮，使你通过**Telnet**访问命令行界面**）

Intelligent Management Switch Manager

System Name	
Object ID	1.3.6.1.4.1.13157.1.2.1.14
Location	
Contact	
System Up Time	0 days, 3 hours, 55 minutes, and 11.59 seconds

Telnet - Connect to textual user interface

Support - Send mail to technical support

Contact - Connect to BITWAY Web Page

命令行界面（CLI） ——指定主机名，位置和联系信息。

```
Switch(config)#hostname bitway 5
Switch(config)#snmp-server location bitway
Switch(config)#snmp-server contact Alan
Switch(config)#exit
Switch#show system
System description: Intelligent Management Switch
System OID string: 1.3.6.1.4.1.13157.1.2.1.14
System information
 System Up time: 0 days, 0 hours, 55 minutes, and 41.84 seco
nds
 System Name              : bitway 5
 System Location          : bitway
 System Contact           : Alan
 MAC address              : 00-30-F1-68-67-40
 Web server               : enable
 Web server port          : 80
 POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test......................PASS
Flash Memory Checksum Test..............PASS
CPU Self Test...........................PASS
MPC850 clock Timer and Interrupt TEST...PASS
WatchDog Timer and Interrupt Test.......PASS
DRAM Test...............................PASS
ACD Chip Test...........................PASS
Switch Driver Initialization............PASS
I2C R/W Test............................PASS
Switch Internal Loopback Test ..........PASS
------------------- DONE --------------------
Switch#
```

设置 IP 地址

交换机的默认 IP **地址未分配。你需要手动配置一个地址，更改交换机的默认设置（**IP **地址是** 0.0.0.0**，子网掩码是** 255.0.0.0**）与网络兼容。你也需要在交换机和存在于另一个网段中的管理站点间建立一个新的默认网关。**

你可以手动配置特定的 IP **地址，或指引设备从** BOOTP **或** DHCP **服务器获取一个地址。有效的** IP **地址由** 4 **个十进制数** 0-255 **组成，用点隔开。**

任何此外的格式 CLI 程序都不接受。

命令属性

- **Management VLAN** ——这是仅有的VLAN，通过VLAN你能获得对交换机的管理访问。默认，所有的端口是VLAN 1的成员，因此管理站点能连接交换机的任何端口。但是如配置其它的VLAN并更改Management VLAN，你将失去对交换机的管理访问的权力。遇此情况，建议再连接管理站点和属于Management VLAN的成员的端口。
- **IP Address Mode**——通过手动配置（静态）、动态主机配置协议（DHCP）或自举协议（BOOTP），指定IP功能性是否被激活。如果DHCP /BOOTP激活，直到从服务器收到回应，IP才会运行。交换机会为IP地址周期性的广播请求。（DHCP /BOOTP的值包括IP地址、子网掩码和默认网关）
- **IP Address**——VLAN界面的地址。有效的IP地址由4个0-255的十进制数字组成，用点隔开。（默认：0.0.0.0）
- **Subnet Mask**——此标记识别主机地址位。（默认：255.0.0.0）
- **Gateway IP Address**——此设备和存在于其它网段中的管理站点间的网关路由器的IP地址。（默认：0.0.0.0）
- **MAC Address**——交换机的物理层地址。

手动配置

Web——点击System，IP。指定管理界面，IP地址和默认网关，然后点击Apply。

IP Configuration

Management VLAN	1
IP Address Mode	Static
IP Address	10.1.0.3
Subnet Mask	255.255.255.0
Gateway IP Address	10.1.0.254
MAC Address	00-55-FF-FF-DD-DD

Restart DHCP

命令行界面——指定管理界面，IP **地址和默认网关。**

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.5 255.255.255.0
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.254
Switch(config)#
```

使用 DNCP/BOOTP

如果网络提供 DNCP/BOOTP **服务，你可以将交换机配置成自动配置。**

Web——点击 System，IP。**指定管理**VLAN，**设置**IP**地址模式为**DHCP**或**BOOTP。**然后点击**Apply **保存更改。点击**Restart DHCP**立即请求一个新的地址。注意交换机将在下一次电源重启时，为**IP**配置设置广播一个请求。**

IP Configuration

Management VLAN	1
IP Address Mode	DHCP
IP Address	10.1.0.3
Subnet Mask	255.255.255.0
Gateway IP Address	10.1.0.254
MAC Address	00-55-FF-FF-DD-DD

Restart DHCP

注意：如果管理连接断开，建议使用控制台连接并输入“ show ip interface **”确定新的交换机地址。**

命令行界面——指定管理界面，设置IP**地址模式为**DHCP**或**BOOTP**。然后输入“** ip dhcp restart **”命令。**

```
Switch(config)#interface vlan 1
Switch(config-if)#ip add dhcp
Switch(config-if)#end
Switch#ip dhcp restart
Switch#show ip interface
 IP address and netmask: 0.0.0.0 255.0.0.0 on VLAN 1,
 and address mode: DHCP.
Switch#
```

更新 DHCP——DHCP **会在一段特定的时间不确定的释放地址给客户端。如果地址满载或交换机被移到其它网段内，你将失去对交换机的管理访问权力。遇此情况，建议重启交换机或递交客户端请求，重启** DHCP **服务。**

Web——如果被 DHCP **分配的地址不再运行，你就不能通过** Web **界面更新** IP **设置。如果当前地址可用，你只能通过** Web **界面重启** DHCP **服务。**
命令行界面——输入以下命令重启 DHCP **服务。**

```
Switch#ip dhcp restart
```

配置用户认证

使用密码或 Radius **菜单限制基于特定用户名的和密码的管理访问。你能手动配置访问权利（密码菜单）,或者使用一个基于** RADIUS **协议（**Radius **菜单）的远程访问认证服务器。**

配置登录密码

客户对大多数配置参数仅有读访问的权力。但管理者有写访问的权力。因此你应该尽快设置一个新的管理者密码，并将密码存放在安全的地方。注意你能重新加载操作代码来恢复默认密码（附录 A **中“通过串口升级固件”有详细描述)。**

默认客名是“ guest **”，密码也是“** guest **”。默认管理者名是“** admin **”，密码为空。注意用户名只能通过** CLI **分配。**

命令属性

User Name*——用户名（最大长度：8**个字符；最多用户数：**5**位）**
Access Level*——指定用户级别（选项：普通和特权）
Password——指定用户密码（最大长度：8**个字符，无格式文本，区分大小写）**
*__仅__CLI

Web——点击 System, Passwords。**输入旧密码，输入新密码，再次输入确认新密码。然后点击**Apply。

Passwords

Old Password	*****
New Password	*****
Confirm Password	********

命令行界面——分配用户名和访问级别15（**如管理者），然后指定密码。**

```
Switch(config)#username alan access-level 15
Switch(config)#username alan password 0 leaf
Switch(config)#
```

配置 RADIUS 登录认证

远程验证拨入用户服务（RADIUS）**是一个登录认证协议。它使用运行在中央服务器上的软件访问符合** RADIUS **标准的网络设备。一个认证服务器包含多个用户名/密码的数据库。**

注意：当 RADIUS **服务器上设置特权级别时，请牢记** 0 **级允许客户（普通访问）访问交换机。只有** 15 **级允许管理者（特权访问）访问。**

命令的使用

通过默认，管理访问总是逆着认证数据库被检验。如果使用远程认证服务器，你必须对远程认证协议指定认证次序和相应的参数。

- RADIUS 使用 UDP，它只提供最佳的发送。
- RADIUS 登录认证通过控制台口、WEB 浏览器或 TELNET 控制了管理访问。这些访问权必须在认证服务器上配置。
- RADIUS 登录认证分配；了一个特定的特权给每个用户名/密码。用户名/密码和特权级别必须在认证服务器上配置。
- 你可以指定一到两个认证方法指出认证次序。例如：如果你选择（1）RADIUS （2）本地，RADIUS 服务器上的用户名和密码首先被校验。如果 RADIUS 服务器不可用，那么本地用户名和密码则被检查。

命令属性

- **Authentication**——选择认证，或认证次序需要：
  - ✧ **Radius**——仅使用 RADIUS 服务器执行用户认证
  - ✧ **Local**——仅使用交换机本地执行用户认证
  - ✧ **Radius, Local**——首先使用 RADIUS 服务器尝试用户认证，然后用交换机本地尝试用户认证。
  - ✧ **Local, Radius**——首先使用交换机本地尝试用户认证，然后用 RADIUS 服务器尝试用户认证。
- **Server IP Address**——认证服务器的地址（默认 10.1.0.1）
- **Server Port Number**——用于认证信息的认证服务器的网络（UDP）端口（范围：1-65535；默认：1812）
- **Secret Text String**——用于认证登录访问客户端的加密密钥。字符串中不能出现空格。（最大长度：20 个字符）
- **Number of Server Transmits**——交换机试图通过认证服务器认证登录访问的次数。（范围：1-30；默认：2）
- **Timeout for a reply**——交换机发送请求前，等待 RADIUS 服务器响应的秒数。（范围：1-65535；默认：5）

注意：通过使用 CLI 手动输入用户名和密码，才能建立本地交换机用户数据库。

Web——点击 System，Radius。**为了配置本地或远程认证参数，指定认证次序（如一到两种方法），填写参数。然后点击** Apply。

Radius Settings

Authentication	Radius
Server IP Address	192.168.1.25
Server Port Number	181
Secret Text String	*****
Number of Server Transmits	5
Timeout for a reply (sec)	10

命令行界面——指定所有需要的参数激活登录认证。

```
Switch(config)#authentication login radius
Switch(config)#radius-server host 192.168.1.25
Switch(config)#radius-server port 181
Switch(config)#radius-server key hello
Switch(config)#radius-server retransmit 5
Switch(config)#radius-server timeout 10
Switch(config)#exit
Switch#show radius-server
Remote radius server configuration:
 Server IP address: 192.168.1.25
 Communication key with radius server: hello
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10
Switch#
```

管理固件

你从 TFTP **服务器上传或下载固件，也可以上传或下载固件到** TFTP **服务器。通过保存运行时间代码到** TFTP **服务器上的文件，日后将这个文件下载到交换机就能恢复操作。**

命令属性

TFTP Server IP Address——TFTP **服务器的** IP **地址**

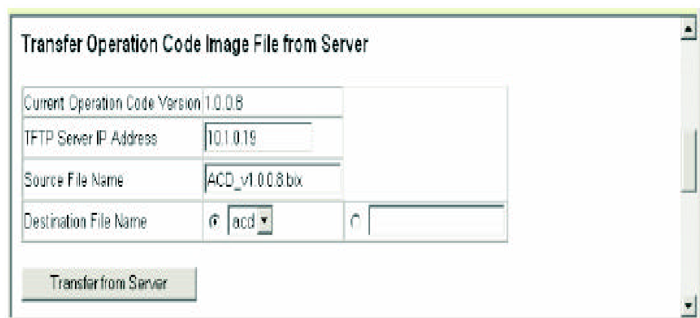
Destination File Name ——文件名不能出现斜杠（/ 或 \），首字母不能是点（.），TFTP**服务器上的文件名的最大长度应小于**127**个字符，交换机上的文件名的最大长度应小于**31**个字符。(有效字符：**A-Z, a-z, 0-9, “.”, “-”, “_”**)**

注意：只有系统软件的副本能保存在交换机的文件目录下。不能删除系统软件文件。

从服务器下载系统软件

当下载运行时间代码时，你必须选择“ Destination File Name **”取代当前值。交换机只能包含一个操作代码文件。**

Web——点击 System，Firmware。**输入**TFTP**服务器的**IP**地址，输入所下载的软件的文件名，输入目的文件名覆盖当前文件，然后点击**Transfer from Sever。**启动新的固件，请重启系统。**



命令行界面——输入T FTP**服务器的**IP**地址，选择**“ config ”**或**“ opcode ”**文件类型。然后输入源和目的文件名，设置新的文件名重启系统，然后重启交换机。**

```
Switch#copy tftp file
TFTP server ip address: 192.168.239.146
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: BS3224TM+v1.0.3.3.bin
Destination file name: BS3224TM+v1.0.3.3.bin
```

保存或恢复配置设置

你可以从 TFTP **服务器上传/下载配置设置，也可以将配置设置上传/下载到** TFTP **服务器。稍后配置文件能被下载恢复交换机设置。**

命令属性

- **TFTP Server IP Address——**TFTP **服务器的** IP **地址**
- **Destination File Name ——文件名不能出现斜杠（** / **或** \ **），首字母不能是点（**.**），**TFTP**服务器上的文件名的最大长度应小于**127**个字符，交换机上的文件名的最大长度应小于**31**个字符。（有效字符：**A-Z, a-z, 0-9,“ .” ,“-”,“ _”）

注意：用户定义的配置文件的最大数目仅受到闪存容量的限制。

从服务器下载配置设置

你能下载配置文件并能将它设置为启动文件，或者你能指定当前启动文件作为目的文件直接代替它。注意名为“ ”的文件能被复制到TFTP **服务器，但是不能用作交换机上的目的文件。**

Web——点击 System，Configuration。**输入**TFTP**服务器的**IP**地址，输入所下载的文件名，选择交换机上的一个文件覆盖当前文件，或指定一个新的文件名。然后点击**Transfer from Sever。

Transfer Configuration File from Server

TFTP Server IP Address	10.1.0.19	
Source File Name	config-1	
Destination File Name	(none)	startup

Transfer from Server

如果你下载一个新的文件名，然后从下拉框中选择新的文件名，点击 Apply Changes。**若要使用新的设置，请重启系统或重启交换机。**

Start-Up Configuration File

File Name startup

Apply Changes

命令行界面——输入TFTP**服务器的**IP**地址，指定服务器上的源文件，设**

置启动文件名，然后重启交换机。

```
Switch#copy tftp startup-config                                    3-14
TFTP server ip address: 10.1.0.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Switch#reload
Switch#
```

如果你下载新的文件名下的启动配置文件。你可以设置此文件为启动文件，然后重启交换机。

```
Switch#config
Switch(config)#boot system config:startup
Switch(config)#exit
Switch#reload
```

重设系统

Web——点击 System，Reset。**点击按钮重启交换机。**



命令行界面——输入reload**命令重启交换机。**

```
Switch#reload
System will be restarted, continue <y/n>?
```

注意：重启系统时，总是会开机自检。

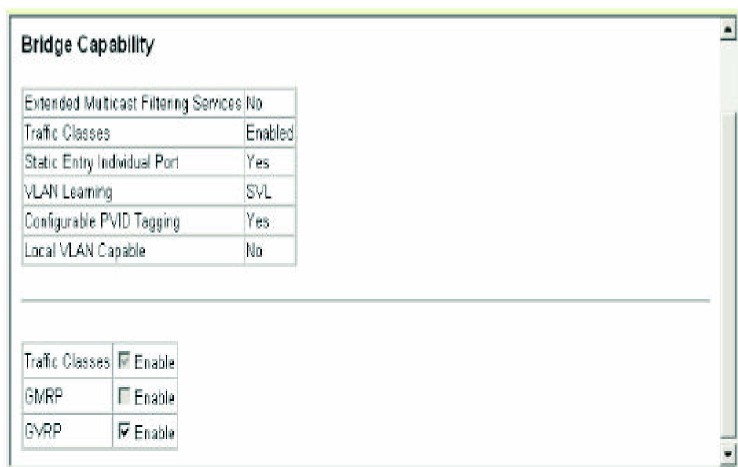
显示网桥扩展性能

网桥MIB**包括对支持多播过滤、数据流级别、虚拟**LAN**的管理型设备的扩展名。你能访问这些扩展名来显示关键变量的默认设置，或对**GARP VLAN**注册协议（**GVRP**）配置全局设置。**

命令属性

- **Extended Multicast Filtering Services——此交换机不支持个别的基于** GMRP（GARP **多播注册协议）的组播地址过滤。**
- **Traffic Classes——此交换机对多个数据流级别提供用户优先级的映射。（参看本章“服务类别的配置”）**
- **Static Entry Individual Port——此交换机允许单播和组播地址的静态过滤（参看本章“设置静态地址”）**
- **VLAN Learning——此交换机使用共享的**VLAN**学习（**SVL**），此处每个端口共享一个普通的过滤数据库。**
- **Configurable PVID Tagging——此交换机允许你不考虑默认端口** VLAN ID**（用于帧标签中的**PVID**）和每个端口的出口状态（**VLAN**—加标签或不加）。（参看本章的“**VLAN**配置”）**
- **Local VLAN Capable——此交换机不支持多个本地网桥。（例：多个生成树）**
- **GMRP——GARP 组播注册协议（GMRP）允许网络设备用组播组来注册终端站点 。交换机不支持 GMRP,它使用 Internet 组管理协议(IGMP)提供自动组播过滤。**
- **GVRP——GARP VLAN 注册协议（GVRP）定义了一种方法使得交换机在网络中通过交换 VLAN 信息来达到在端口上自动注册 VLAN 成员的目的。建议激活此功能，许可 VLAN 组。(默认：激活)**

Web——点击 System，Bridge Extension。


Bridge Capability

Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Learning	SVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

Traffic Classes	☑ Enable
GMRP	☐ Enable
GVRP	☑ Enable

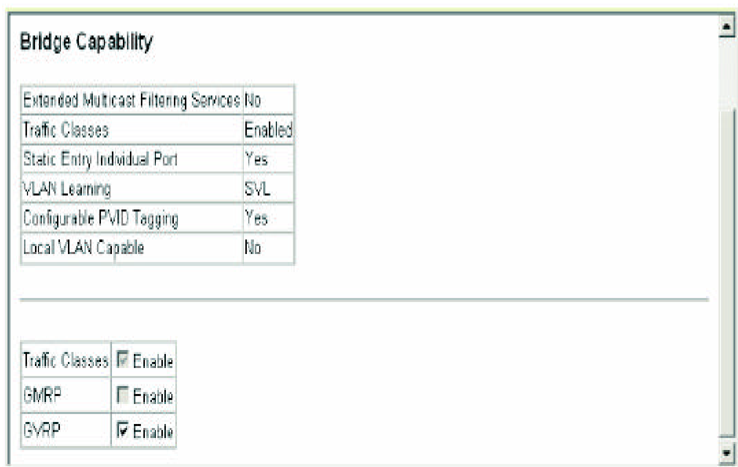
命令行界面——输入下列命令。

```
Switch#reload
System will be restarted, continue <y/n>? n
Switch#
Switch#show bridge-ext
 Max support vlan numbers: 127
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: SVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Disabled
 GMRP: Disabled
Switch#
```

激活或禁用 GVRP（全局设置）

GVRP VLAN 注册协议（GVRP）定义一种方法使得交换机在网络中通过交换 VLAN 信息来达到在端口上自动注册 VLAN 成员的目的。基于由主机设备发放并传遍整个网络的信息，VLAN 被动态配置。激活 GVRP 才能自动完成 VLAN 注册，并支持 VLAN。（默认：激活）

Web——点击 System，Bridge Extension。激活或禁用 GVRP，点击 Apply。



命令行界面——下例对交换机激活了 GVRP。

```
Switch(config)#bridge-ext gvrp
Switch(config)#
```

显示激活就硬件/软件版本

使用交换机信息页显示主板和管理软件的硬件/软件版本号，和系统的电源状态。

命令属性

主板

- **Serial Number——交换机的序列号**
- **Number of Ports——交换机的端口数**
- **Hardware Version——主板的硬件版本**
- **Internal Power Status——显示内部供电状态**

管理软件

- **Loader Version——装入程序代码的版本号**
- **Boot-ROM Version——开机自检和引导程序代码的版本号**
- **Operation Code Version——运行时间代码的版本号**
- **Role——显示交换机是主机（例：独立操作）**

扩展插槽

- **Expansion Slot——显示任意已安装的模块类型**

Web ——点击 System，Switch Information。

Main Board:

Serial Number	12345
Number of Ports	26
Hardware Version	012
Internal Power Status	Active

Management Software:

Loader Version	1.0.0.1
Boot-ROM Version	1.0.0.1
Operation Code Version	1.0.0.8
Role	Master

Expansion Slot:

Expansion Slot 1	Not Present
Expansion Slot 2	Not Present

命令行界面——使用以下命令显示版本信息。

```
Switch#show version
Unit1
 Serial number          :
 Hardware version       :
 Module A type          :1000Base-LX-SC SMF
 Module B type          :1000Base-SX-SC MMF
 Number of ports        :26
 Main power status      :up
Agent(master)
 Unit id                :1
 Loader version         :1.0.0.3
 Boot rom version       :1.0.0.3
 Operation code version :1.0.3.3
Switch#
```

端口配置

显示连接状态

你可以使用端口信息和 Trunk 信息页来显示当前连接状态，包括速率/双工模式，流量控制和自适应。

命令属性

- NAME——接口标签。
- TYPE——显示端口类型。（100BASE-TX，1000BASE-T，1000BASE-SX，1000BASE-LX，100BASE-FX）
- ADMIN STATUS——显示接口是被激活或是禁止。
  WEB——显示激活或是禁止
  CLI——显示端口管理
- LINK STATUS——显示连结是上还是下（仅 CLI）
- OPER STATUS——显示连结是上还是下（仅 WEB）
- PORT OPERATION STATUS——提供端口状态的详细信息。
  仅 CLI；显示它的项是上还是下
- SPEED/DUPLEX STATUS——显示当前的速率和双工模式
- FLOW CONTROL STATUS——显示当前使用的流量控制类型
  WEB——IEEE 802.3x，背压或无
  CLI——激活或禁用。流量控制类型显示 IEEE 802.3x，背压或无
- AUTPNEGOTIATION——显示自适应是否被激活
- MAC ADDRESS——端口的物理层地址
  仅 CLI；若要在 WEB 上访问，参看本章“设置 IP 地址”
- TRUNK MEMBER——显示端口是否是 TRUNK 的成员（仅端口信息）

- CREATION——显示一个 TRUNK 是否是手动配置的（仅 TRUNK 信息）
- PORT Capabilities——在自适应期间对指定端口广播性能。支持以下性能：
  - ✧ 10half——支持 10Mbps 半双工操作
  - ✧ 10full——支持 10Mbps 全双工操作
  - ✧ 100 half——支持 100Mbps 半双工操作
  - ✧ 100full——支持 100Mbps 全双工操作
  - ✧ 1000full——支持 1000Mbps 全双工操作
  - ✧ Syn——对流量控制发送并接收暂停帧
  - ✧ FC——支持流量控制

Web——点击端口，端口信息或 TRUNK 信息。

Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Trunk Member
1		100Base-TX	Enabled	Up	100full	IEEE 802.3x	Disabled	
2		100Base-TX	Enabled	Down	10half	None	Enabled	
3		100Base-TX	Enabled	Down	10half	None	Enabled	
4		100Base-TX	Enabled	Down	10half	None	Enabled	
5		100Base-TX	Enabled	Down	10half	None	Enabled	

命令行界面——下例显示了端口 13 的连接状态。

```
Switch#show interfaces status ethernet 1/25
Information of Eth 1/25
 Basic information:
  Port type: 1000LX
  Mac address: 00-30-F1-68-67-59
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: 1000full
  Capabilities: 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 6 percent
  Flow control: Disabled
 Current status:
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: None
Switch#
```

配置接口连接

你可以使用 TRUNK 配置或是端口配置页来激活或是禁用一个端口，手动的配置速率和双工模式，设定流量控制和自动流通，还能设定接口的通告容量。

命令属性

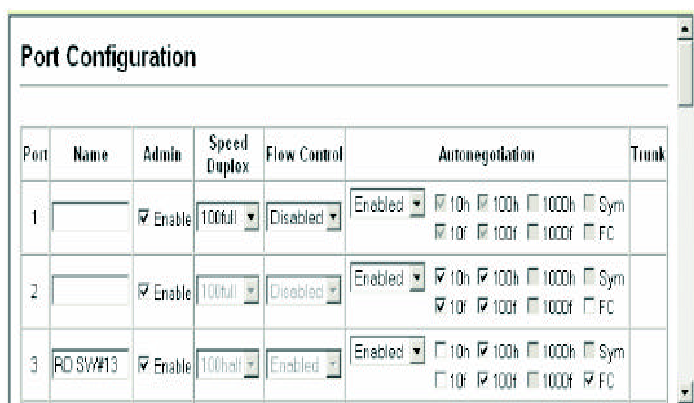
- NAME——允许你标注一个接口。（范围：1-64 字符）
- ADMIN——允许你手动的禁用一个接口。你能够由于不正常的动作来禁用一个接口，然后再问题解决之后再重新激活它。你也可以由于安全原因来禁用一个接口。
- SPEED/DUPLEX——允许手动的为端口选择速度和双工模式。
- FLOW CONTROL——允许自动激活或禁用流量控制。

- AUTONEGOTIATION（PORT CAPABILITIES）——允许自适应被禁止或是激活。当自适应激活时，需要指定性能被通告。当自适应禁用时，能强行设置速率、模式、流量控制。能支持下列性能。
  - ✧ 10half——支持 10Mbps 半双工操作。
  - ✧ 10full——支持 10Mbps 半双工操作。
  - ✧ 100half——支持 100Mbps 半双工操作。
  - ✧ 100full——支持 100Mbps 全双工操作。
  - ✧ 1000full——支持 1000Mbps 全双工操作。
  - ✧ SYM（仅千兆）——发送和接收流量控制的暂停帧；或清除它，实现非均衡暂停帧与发送器或接受器自动协商。（目前交换机芯片仅支持均衡暂停帧）
  - ✧ FC——支持流量控制。

  流量控制可以消除由于交换机缓冲器充满而导致流量堵塞而引起的数据帧丢失的现象。当激活后，背压用于半双工操作，IEEE802.3x 用于全双工操作。（当一个端口被连到集线器上时，不该使用流量控制，除非它确实需要解决一个问题。否则背压干扰信号将会削弱这个网段的性能。）
- TRUNK——显示一个端口是否是 TRUNK 的成员。若要创建 TRUNK 并选择端口成员，参看本章“端口 TRUNK 配置”。

*注意：在你能够配置或强迫这个接口使用速度/双工模式或流量控制前，自适应必须被禁用。

Web——点击端口，TRUNK **配置或端口配置。修改需要的端口设置，然后点击** Apply。



命令行界面——选择 interface，然后输入所需的设置。

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#description bitway
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
Switch(config-if)#no negotiation
Switch(config-if)#speed-duplex
% Incomplete command.
Switch(config-if)#speed-duplex 100half
Switch(config-if)#capabilities 100half
Switch(config-if)#capabilities 100full
Switch(config-if)#capabilities flowcontrol
Switch(config-if)#
```

设置广播风暴的域值

当网络中的设备出现故障时或如果没有很好的设计或正确配置应用程序时，可能会引起广播风暴。如果网络中有太多的广播数据流，性能将大大降低，每件设备都可能完全停止。

通过对每个端口的广播数据流设置一个域值，你就能保护你的网络不受广播风暴的侵害。任何超过指定域值的广播数据包将被丢弃。

命令的使用

- **广播风暴控制默认为激活**]
- **默认阈值是端口带宽的** 6%
- **广播控制不影响** IP **多播数据流**

命令属性

- **Type ——显示端口类型** (100BASE-TX, 1000BASE-T, 1000BASE-SX,1000BASE-LX 100BASE-FX)
- **Protect Status——显示广播风暴控制在此端口是否激活（默认：激活）**
- **Threshold——阈值是端口带宽的百分比** (**选项：**6%, 20%**；默认：**6%)
- **Trunk——显示端口是否是** TRUNK **的成员。若要创建** TRUNK **并选择端口成员，参看本章“端口** TRUNK **配置”。**

Web——打开系统，点击端口，端口广播控制或 TRUNK **广播控制。对每个端口或** TRUNK **设置域值，然后点击** Apply。

Port Broadcast Control

Port	Type	Protect Status	Threshold (6% or 20%)	Trunk
1	100Base-TX	☑ Enable	6	
2	100Base-TX	☑ Enable	6	
3	100Base-TX	☑ Enable	20	
4	100Base-TX	☑ Enable	6	
5	100Base-TX	☑ Enable	6	1

命令行界面——指定所需的接口，然后输入阈值。下例对端口 3 **设置了广播抑制端口为端口带宽的** 20%。

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#switchport broadcast percent 20
Switch(config-if)#end
Switch#show interface switchport ethernet 1/5
Information of Eth 1/5
 Broadcast threshold: Enabled, 20 percent
 Ingress rate limit: Disabled
 Egress rate limit: Disabled
 VLAN membership mode: Access
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
 Private-vlan mode: NONE
 Private-vlan host-association: NONE
 Private-vlan mapping: NONE
Switch#
```

配置端口镜像

你可以镜像任何源端口的数据流量到目的端口以便于实时分析。你可以连结一个逻辑分析仪或是 RMON 探测器到目的端口以完全不冲突的方式研究通过源端口的数据。

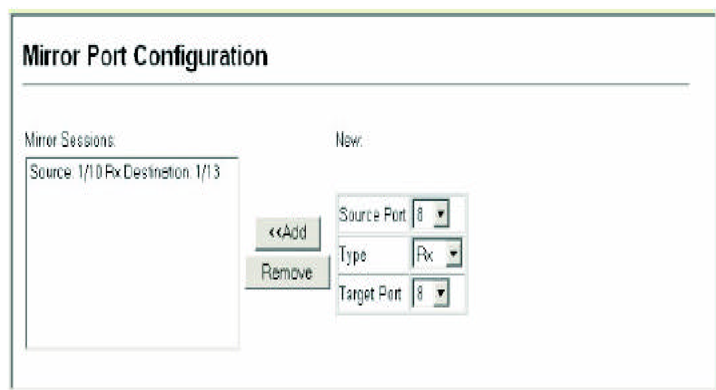
命令的使用

- 镜像端口和监控端口的速率必须匹配，否则数据可能从镜像端口丢失。
- 所有的镜像会话必须共享同一个目的端口
- 当镜像端口数据流时，目标端口必须被包括在相同的 VLAN 中作为源端口。

命令属性

- Mirror Sessions——显示当前镜像会话
- Source Port——此端口的数据流将被镜像
- Type——使你能选择数据流镜像到目标端口，Rx（接收），Tx（发送），或同时选用两种类型
- Target Port——端口将在源端口上“复制”或“镜像”数据流

Web——点击端口，镜像，指定源端口，被镜像的数据类型和镜像端口，然后点击 Add。



命令行界面——使用界面命令选择镜像端口，然后使用端口镜像命令指定源端口。注意命令行界面下的默认镜像同时针对已发送或已接收的数据包。

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#port monitor ethernet 1/10
Switch(config-if)#
```

地址表设置

交换机为所有已知的设备保存地址。此信息用于在输入、输出端口间直接路由数据流。监控数据流获知的所有地址被保存在动态地址表中。你也可以手动配置特定端口的态地址。

设置静态地址

静态IP地址能被分配到交换机上的特定界面。静态地址分配到界面将不会被移动。当静态地址出现在另一个界面上，地址将被忽略，不会被写入地址表。

命令属性

- **Static Address Counts*——手动配置的地址数目**
- **Current Static Address Table——列出所有的静态地址**
- **Mode——显示有目的地址的数据包是否会被转发或丢弃**
- **Interface——端口或与设备相关的** TRUNK **分配一个静态地址**
- **MAC Address——映射到此界面设备的物理地址**
- **Duration——地址能被设置为以下类型：**
  - ✧ **Permanent——分配是永久的，在交换机重启后被存储**
  - ✧ **Delete on Reset——交换机重启前，持续分配**

***仅** Web

Web——点击 Address Table，Static Addresses。**指定模式，界面，**MAC**地址和持续时间，然后点击**Add Static Address。

Static Addresses

Static Address Counts	1	
Current Static Address Table	00-E0-29-94-34-DE, Unit 1, Port 3, Permanent	
Mode	Forward	
Interface	Port 1	Trunk 1
MAC Address		
Duration	Delete on Reset	

Add Static Address | Remove Static Address

命令行界面——下例添加了一个地址到静态地址表，默认设置为永久。

Switch(config)#mac-address-table static 00-e0-29-93-34-de interface Ethernet 1/5

Switch(config)#

显示地址表

动态地址表包含 MAC **地址。当发现数据库中输入数据流的目标地址时，针对那个地址的数据包直接被转发到相应的端口。否则，数据流会泛洪到所有的端口。**

命令属性

- **Interface——显示端口或** TRUNK

- **MAC Address——与此接口相关的物理地址**
- **Address Table Sort Key——你能对基于界面（端口或**TRUNK**）或**MAC **地址的显示的信息进行分类**

Web——点击 Address Table，Dynamic Addresses。**指定搜索类型（例：** mark the Interface，MAC Address checkbox），**选择分类方法，然后点击** Query。

Dynamic Addresses

Query by:

Interface Port 1 Trunk 1

MAC Address

Address Table Sort Key Address

Query

Dynamic Address Table

Dynamic Address Counts

Current Dynamic Address Table 00-10-B5-62-03-74, Unit 1, Port 1, Dynamic

命令行界面——下例显示了端口 1 **的地址表键值。**

```
Switch#sh mac-address-table interface ethernet 1/5 sort address
 Interface Mac Address       Type
 --------- ----------------- --------------------
  Eth 1/ 5 00-E0-29-94-23-CD Permanent
Switch#
```

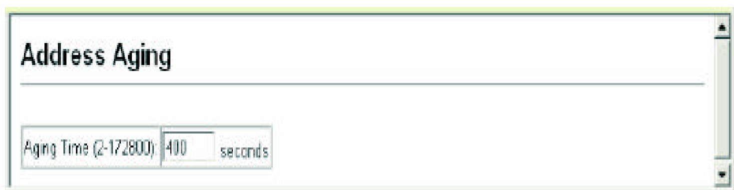
更改老化时间

你能在动态地址表中对键值设置老化时间。

命令属性

- Aging Time——**学习的键值被丢弃后的时间。（范围：**2-172800 **秒；默认：**300 **秒）**

Web——点击 Address Table ，Address Aging。**定义新的老化时间，然后点击**Apply。



命令行界面——下例设置了老化时间为 400 **秒。**

```
Switch(config)#mac-address-table aging-time 400
Switch(config)#
```

生成树算法的配置

生成树算法（STA**）能用于侦测并禁用网络循环，在交换机、网桥或路由器间提供备份连接。这使交换机能够和其它网桥设备相联系（即：**STA **兼容的交换机、网桥或路由器），确保只有一个路由器存在于任意两个网络站点间，并提供备份连接（原来的连接下来时自动接管）。**

管理全局的设置

全局设置适用于整个交换机。

命令属性

下列全局属性只读不可更改。

- Bridge ID——这台设备的优先级和MAC地址。
- Designated Root——在生成树协议中这台设备的优先级和MAC地址，交换机已经接受根设备。
- Root Port——靠近此根的交换机端口数目。这台交换机通过此端口与根设备通信。如果没有根端口，则已经接受交换机作为生成树网络的根设备。
- Root Path Cost——从这台交换机的根端口到根节点设备的路径成本。

以下的全局属性显示了统计的值，不能更改：

- Configuration Changes——生成树被重新配置的次数。
- Last Topology Change——生成树备最后一次重新配置过之后的时间。
- Hold Time——连续的 BPDU 配置（仅 CLI）间传输最小的时间间隔。

以下的全局属性是可以被配置的：

- Spanning Tree State——激活或禁止这台交换机参与 STA 兼容的网络。
- Priority——在选择根节点设备，根端口和和指定端口时所用到的桥路优先级。由最高的优先级的设备成为STA根节点设备，但是如果所有的设备有着相同的优先级，那么MAC地址最小的设备成为根节点设备。

—默认：32768

—范围：0-65535

- **Hello Time**——根节点设备发出配置信息的时间间隔（秒）。

—默认：2

—最小值：1

—最大值：10 或[(最大消息时间/2）-1]之间的较小值

- **Maximum Age**——一个设备在尝试再次配置前没有接收到配置信息所能等待的最大时间。所有的设备端口应该在规则的间隔内收到配置信息，任何一个给出 STA 信息的端口将成为对应的 LAN 的指定端口，如果他是一个根端口，就从相关联的设备端口中重新选择一个根端口。

—默认：20

—最小值：6 和[（问候时间+1）×2]之间的较大值

—最大值：40 和[（前向延迟-1）×2]之间的较小值

- **Forward Delay**——在改变状态前根节点设备所能等候的最大时间（秒）。这种延迟是必需的，因为每个设备开始转发帧之前，它必须接受拓扑更改信息。此外，每个端口都需要时间来学习可能是它返回到阻塞状态的冲突信息；否则可能会产生临时数据环路。

—默认：15

—最小值：4 和[（最大消息时间/2+1）]之间的较大值

—最大：30

对 STA 显示全局设置

Web——点击 Spanning Tree，STA，STA Information。

STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0030F154F880
Bridge ID	32768.0055FFFFDDDD	Root Port	2
Max Age	20	Root Path Cost	18
Hello Time	2	Configuration Changes	5
Forward Delay	15	Last Topology Change	0 d 1 h 57 min 5 s

命令行界面——此命令显示全局 STA 设置，按照每个端口的设置。

```
Switch#show spanning-tree
Bridge-group information
--------------------------------------------------------------
 Spanning tree protocol              :IEEE Std 802.1D
 Spanning tree enable/disable        :enable
 Priority                            :32768
 Hello Time (sec.)                   :2
 Max Age (sec.)                      :20
 Forward Delay (sec.)                :15
 Designated Root                     :32768.0030F1686740
 Current root port                   :0
 Current root cost                   :0
 Number of topology changes          :0
 Last topology changes time (sec.):12116
 Hold times (sec.)                   :1
---------------------------------------------------------------
Eth  1/ 1 information
--------------------------------------------------------------
 Admin status          : enable
 STA state             : broken
 Path cost             : 100
 Priority              : 128
 Designated cost       : 0
 Designated port       : 128.1
 Designated root       : 32768.0030F1686740
 Designated bridge     : 32768.0030F1686740
 Fast forwarding       : disable
 Forward transitions   : 0
Eth  1/ 2 information
```

注意：当这个设备不连接网络时，当前根端口和当前根值显示为 0。

对 STA 配置全局设置

Web——点击 Spanning Tree，STA Configuration。**更改所需的属性，然后点击** Apply。

STA Configuration

Switch:

Spanning Tree State	Enabled
Priority	40000

When the Switch Becomes Root:

Hello Time(1-10)	5	seconds
Maximum Age(6-40)	40	seconds
Forward Delay(4-30)	20	seconds

命令行界面——此例激活了生成树协议，然后设置显示的属性。

```
Switch(config)#spanning-tree
Switch(config)#spanning-tree priority 40000
Switch(config)#spanning-tree hello-time 5
Switch(config)#spanning-tree max-age 20
Switch(config)#spanning-tree forward-time 20
Switch(config)#
```

管理 STA 界面设置

你能对特定的界面配置 STA 属性，包括端口优先级，路径成本和快速转存。你可以对相同媒质类型的端口使用不同的优先级或路径成本，来显示首选路径。

命令属性

以下属性只读不可更改：

- **Port Status——在生成树中，显示当前端口状态。**
  - ✧ **Disabled——此端口没有建立连接。否则，此端口被用户禁用或诊断失败。**
  - ✧ **Blocking——端口接收** STA **配置信息，但不转发数据包。**
  - ✧ **Listening——由于拓扑更改端口将离开阻塞状态，开始传输配置信息，但不转发数据包。**
  - ✧ **Learning——端口在一段时间间隔已经传输配置信息，时间间隔被** Forward Delay **参数设置，不接收反对信息。端口地址表被清除，端口开始学习地址。**
  - ✧ **Forward——端口转发数据包并继续学习地址。**
  - ✧ **Broken——端口正在出现或没有建立连接**

定义端口状态的规则是：

- ➢ **网段上的端口如没有遵从其他** STA **桥接设备，总是会被转发。**
- ➢ **如果交换机的两个端口连接到相同的网段，而且没有其他** STA **设备连接到此网段，有较小** ID **的端口转发数据包，其他的则被阻塞。**
- ➢ **当交换机被启动时，所有的端口被阻塞，其中一些端口改变状态为侦听、学习，然后转发。**

- Forward Transitions——端口已经从学习状态转换到转发状态的次数
- Designated Cost——数据包的值传播到端口的根。媒质越慢，值越高
- Designated Bridge——设备 MAC 地址的优先级，通过它，端口必须传达到生成树的根
- Designated Port——端口的数目和优先级，通过它，交换机必须用生成树的根进行通信
- Trunk Member——显示端口是否是 TRUNK 的成员（仅 STA 端口信息）

下列界面属性可以被配置

- Priority——定义在生成树协议下用于端口的优先级。如果路径成本相同，有最高优先级（例：最低值）的端口作为活动连接被配置。如果生成树协议正侦测网络循环，这使更高优先级的端口不容易被阻塞。

不止一个端口被分配了最高优先级的地方，有最低数字标识符的端口将被激活。

—默认：128

—范围：0～255

- Path Cost——此参数被 STP 用于决定设备间最好的路径。因此低些的值应该被分配给连在更快媒质的端口，高些的值应该被分配给连在慢一些的媒质的端口。（路径成本在端口优先级上有优先权）
  - ✧ 全部范围：1-65535
  - ✧ 建议范围：
    - —以太网：50-600

—快速以太网：10-6

—千兆以太网：3-10

✧ **默认：**

—以太网—半双工：100；**全双工**：95；trunk：90

—快速以太网—半双工：19；**全双工**：18；trunk：15

—千兆以太网—全双工：4；trunk：3

- **Fast forward——由于终端节点不能引起转发循环，它们能通过转发状态被直接传输。快速转发能为终端节点和服务器完成更快的集中，也能克服其它有关超时问题的** STA。**（切记：只能对连接终端节点的设备的端口激活快速转发）**

  ✧ **默认：禁用**

对 STA 显示界面设置

Web——点击 Spanning Tree, STA Port Information **或** STA Trunk Information。

STA Port Information

Port	Port Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Trunk Member
1	Forwarding	2	18	32768.0055FFFFDDDD	128.1	
2	Forwarding	2	0	32768.0030F154F880	128.11	
3	Broken	0	18	32768.0055FFFFDDDD	128.3	
4	Broken	0	18	32768.0055FFFFDDDD	128.4	
5	Broken	0	18	32768.0055FFFFDDDD	128.33	1
6	Broken	0	18	32768.0055FFFFDDDD	128.6	

命令行界面——此例显示了对端口1**的**STA**属性。**

```
Switch#show spanning-tree ethernet 1/5
Bridge-group information
--------------------------------------------------------------
 Spanning tree protocol              :IEEE Std 802.1D
 Spanning tree enable/disable        :enable
 Priority                            :40000
 Hello Time (sec.)                   :5
 Max Age (sec.)                      :20
 Forward Delay (sec.)                :20
 Designated Root                     :40000.0030F1686740
 Current root port                   :0
 Current root cost                   :0
 Number of topology changes          :0
 Last topology changes time (sec.):12467
 Hold times (sec.)                   :1
---------------------------------------------------------------
Eth  1/ 5 information
--------------------------------------------------------------
 Admin status            : enable
 STA state               : broken
 Path cost               : 19
 Priority                : 128
 Designated cost         : 0
 Designated port         : 128.5
 Designated root         : 40000.0030F1686740
 Designated bridge       : 40000.0030F1686740
 Fast forwarding         : disable
 Forward transitions     : 0
Switch#
```

对 STA 配置界面设置

Web——打开 Spanning Tree, STA Trunk Configuration **或** STA Port Configuration。**更改所需的属性，然后点击** Apply。

STA Port Configuration

Port	Type	STA State	Priority	Path Cost	Fast Forwarding	Trunk
1	100Base-TX	Forwarding	0	50	☑ Enabled	
2	100Base-TX	Forwarding	128	18	☐ Enabled	
3	100Base-TX	Broken	128	100	☐ Enabled	
4	100Base-TX	Broken	128	100	☐ Enabled	
5	100Base-TX	Broken	128	90	☐ Enabled	1
6	100Base-TX	Broken	128	100	☐ Enabled	

命令行界面——此例显示了对端口 5 **的** STA **属性。**

Switch(config)#interface ethernet 1/5

Switch(config-if)#spanning-tree port-priority 0

Switch(config-if)#spanning-tree cost 50

Switch(config-if)#spanning-tree portfast

VLAN 的配置

在传统的使用路由器的网络中，广播通信被分为隔离的域。交换机本身不支持域中的广播，这就有可能在大型网络中处理 IPX 和 NetBeui **协议时导致广播风暴。通过使用 IEEE802.1Q 兼容的 VLAN，你可以将任何网络节点的组合组织成分离的广播域，这样可以限制向原始组的流量。这也提供了一个更加安全和干净的网络环境。**

一个 IEEE802.1Q VLAN 是由一组可以位于网络中任何位置的端口的组合，但是它们却可以像在一个物理网段中进行通信。

VLAN 允许你对网络的物理连接不做任何改动而把设备移到其它的 VLAN 中以简化网络管理。VLAN 能够被简单的组织以反映部门的组，使用组和组播组。

VLAN 通过减少广播流量以提高网络效率，并且允许你不用改动 IP 地址和子网 IP 来做网络改动。VLAN 内在的提供了一个高层的网络安全因为数据必须通过一个配置过的第三层连接以到达另外的一个 VLAN。

- 基于 IEEE802.1Q 标准的多达 127 个 VLAN
- 通过多个使用内在的和外在的标记和 GVRP 协议的交换机的分布式学习功能。
- 端口叠加，允许一个端口参与多个 VLAN
- 终端站能够属于多个 VLAN
- 在认识 VLAN 和不认识 VLAN 的设备中进行数据通信。
- 优先权标记

给 VLAN 分配端口

在对交换机 VLAN 激活之前，你必须将每个端口分配到它所属于的 VLAN 中。默认是所有的端口以无标记方式被分配给了 VLAN 1，如果你想让一个端口在不同的 VLAN 中运载数据而且另外一端的连接也是支持 VLAN 的，你应该将它设置为带标记端口。另外，如果你想让这台交换机上的一个端口参与多个 VLAN 的话，但是另一端的联接的设备不支持 VLAN，这时，这个端口应该被设置为无标记端口。

VLAN 的分类——如果一台交换机收到了一个数据帧，它将以两种方式之一来分类这个数据帧。如果这个数据帧是没有标记的，那么交换机根据 VLANID 把这个数据帧分配到特定的 VLAN;如果这个数据帧是标记的，交换机就会用这个标记过的 VLANID 来区分这个端口的广播域。

端口叠加——端口叠加被用来在不同的 VLAN 组中对共享的网络资源进行访问，象文件服务器和打印服务器。注意，如果你想利用没有叠加的 VLAN

来进行数据通信，你可以利用一个第三层的交换机或者是路由器来联结他们。

基于端口的 VLAN——基于端口的 VLAN 是手动地连接到特定的端口。交换机的前向目的是基于 MAC 地址和相关联的端口。因此为了做出有效的前向传送决定，交换机必须能够学习 MAC 地址和相关端口的关系，并且实时的传送到 VLAN。但是，当 GVRP 协议被激活时，这个过程可以是完全自动的。

自动 VLAN 注册——GVRP（GARP VLAN 注册协议）定义了一个系统说明为什么交换机能够自动的学习到每台终端机应该分配给哪一个 VLAN。如果一台终端机（或网络适配器）支持 IEEE 802.1Q VLAN 协议，它可以被配置成向网络中它想要加入的 VLAN 发出广播信息。当交换机接收到这些信息时，他会自动的在 VLAN 中选择接收端口，然后向所有的端口发送这个消息。当消息到达支持 GVRP 协议的另外一台交换机并且向所有的其它端口发送消息时，VLAN 的要求以这种方式在网络传播。
为了在一个网络中应用 GVRP，你必须首先配置连接到电脑，服务器和其它设备上的交换机所要求的静态 VLAN，因此这些 VLAN 能够在网络中被传播。对于在网络中的其它核心交换机，在交换机这些设备的连接中激活 GVRP 协议。你也应该决定网络中的安全边界，禁止端口的 GVRP 以禁止通告被传播，或者禁止限制 VLAN 中的端口。

转发标记/未标记数据帧
如果你想为只与一个交换机连接的设备创建一个小的基于端口的 VLAN，你可以为同一个无标记 VLAN 分配端口。但是，如果要参与进一个包括几台交换机的 VLAN，你就应该为这个组建立一个 VLAN 并且以标记的方式激

活所有端口。

端口可以被分配给多个加标记和没有加标记的 VLAN 中，交换机上的每一个端口因此能够传输加标记或是没有加标记的数据帧。为了能从一个支持 VLAN 的设备转发数据帧到一个不支持 VLAN 的设备上，这台交换机首先应该决定向哪里传送数据帧，然后拨去数据中的标记。但是，如果从一台不支持 VLAN 的设备向一台支持 VLAN 的设备上转发数据帧的话，这台交换机首先应该决定向哪里传送数据帧，然后再加入一个 VLAN 标记以反映出这个端口的默认 VID。

显示基本的 VLAN 信息

VLAN 基本信息页显示有关 VLAN 类型的基本信息。

命令属性

- **VLAN Version Number***——由 IEEE 802.1 标准规定的这台交换机所用的 VLAN 版本号。
- **Maximum VLAN ID**——经过交换机验证的最大的 VLAN ID。
- **Maximum Number of Supported VLANs**——这台交换机所能配置的最大 VLAN 数目。

Web——点击 VLAN，VLAN 基本信息。

VLAN Basic Information

VLAN Version Number	1
Maximum VLAN ID	4094
Maximum Number of Supported VLANs	127

命令行界面——请输入以下命令。

```
Switch#show bridge-ext
 Max support vlan numbers: 127
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: SVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Switch#
```

显示当前的 VLAN

命令属性（WEB）

- **VLAN ID——配置的** VLAN **的** ID。（1-4094）
- **Up Time at Creation——这个** VLAN **被创建的时间（例：系统上电时间。）**
- **Status——显示这个** VLAN **是怎样被加到交换机上的。**
  —Dynamic GVRP——通过 GVRP **自动学习。**
  —Permanent——以静态接口被加入。
- **Tagged Ports——显示带标记的** VLAN **端口成员。**
- **Untagged Ports——显示无标记端口成员。**

Web——点击 VALN，VLAN 当前菜单。从下拉菜单中选择任何 ID。

VLAN Current Table

VLAN ID: 1

Up Time at Creation	0 d 0 h 0 min 7 s
Status	Permanent

Egress Ports: Unit1 Port1, Unit1 Port2, Unit1 Port3, Unit1 Port4, Unit1 Port6, Unit1 Port7, Unit1 Port8, Unit1 Port9

Untagged Ports: Unit1 Port1, Unit1 Port2, Unit1 Port3, Unit1 Port4, Unit1 Port6, Unit1 Port7, Unit1 Port8, Unit1 Port9

命令属性（CLI）

- **VLAN ID——配置的** VLAN **的** ID(1-4094)。
- **Type——显示** VLAN **如何被添加到交换机。**

  —Dynamic：自动通过 GVRP **学习。**

  —Static：作为一个静态键值被添加。
- **Name——**VLAN **的名称（不超过** 15 **个字符）。**
- **Status——显示这个** VLAN **时被激活还是被禁止。**

  活动——VLAN **正在运行。**

  延缓——VLAN **被延缓。**
- **Ports / Channel groups——显示**VLAN**接口的成员。**

命令行界面——当前的 VLAN **信息用如下命令能被显示。**

```
Switch#show vlan id 1
VLAN Type     Name              Status    Ports/Channel groups
---- -------- ----------------- --------- --------------------------------
----------
   1  Static       DefaultVlan     Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4
 Eth1/ 5
                                          Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9
 Eth1/10
                                          Eth1/11 Eth1/12 Eth1/13 Eth1/14
 Eth1/15
                                          Eth1/16 Eth1/17 Eth1/18 Eth1/19
 Eth1/20
                                          Eth1/21 Eth1/22 Eth1/23 Eth1/24
 Eth1/25
                                          Eth1/26
Switch#
```

创建 VLAN

使用 VLAN 静态列表创建或除去 VLAN 组。要将有关 VLAN 组的信息传播到外部网络设备，你必须对每个组指定一个 VLAN ID。

命令属性

- **Current——列出所有为此系统创建的当前 VLAN 组。能定义多达 127 个 VLAN 组。VLAN1 是默认未标记的 VLAN。**
- **New——允许你指定相同的名字和数字标识符。（VLAN 名仅用于系统的管理；不添加到 VLAN 标记）**
- **VLAN ID——配置的 VLAN 的 ID(1-4094)。**
- **VLAN Name——VLAN 的名字（1-32 个字符）。**
- **Status（Web）——显示这个 VLAN 时被激活还是被禁止。**

  激活——VLAN 正在运行。

  禁止——VLAN 被挂起。
- **State（CLI）——显示 VLAN 时被激活还是被禁止。**

  活动——VLAN 正在运行。

延缓——VLAN 被延缓。

- Add——添加一个新的 VLAN 组到当前列中。
- Remove——从当前列中除去一个 VLAN 组。如果任何端口被分配到这个作为未标记，它将被重新分配到 VLAN 组作为未标记。

Web——点击 VLAN，VLAN 静态列表。输入 VLAN ID 和 VLAN 名字，标记 Enable 检验栏以激活 VLAN，然后点击 Add。

VLAN Static List

Current:
1. DefaultVlan, Enabled

<<Add
Remove

New:
VLAN ID (1-4094) 2
VLAN Name R&D
Status ☑ Enable

命令行界面——此例创建了一个新的 VLAN。

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2 name bitway media ethernet state active
Switch(config-vlan)#end
Switch#show vlan
VLAN Type     Name                Status     Ports/Channel groups
---- -------- ---------------- --------- ----------------------------------
---------
   1  Static       DefaultVlan     Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4
 Eth1/ 5
                                          Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9
 Eth1/10
                                          Eth1/11 Eth1/12 Eth1/13 Eth1/14
 Eth1/15
                                          Eth1/16 Eth1/17 Eth1/18 Eth1/19
 Eth1/20
                                          Eth1/21 Eth1/22 Eth1/23 Eth1/24
 Eth1/25
                                          Eth1/26
   2  Static            bitway     Active
Switch#
```

添加静态成员到 VLAN

命令属性

- VLAN——配置的 VLAN 的 ID（1-4094）。
- NAME——VLAN 的名称（1-32 个字符）。
- STATUS——显示 VLAN 是被激活还是被禁止。

  —ENABLE——VLAN 在运行。

  —DISABLE——VLAN 被延缓。如：不传输数据包。
- PORT——端口标识符。
- TRUNK——trunk 标识符。
- MEMBER TYPE——标记一个端口或 trunk 标记适当的按钮来对每一个接口选择 VLAN 的成员。

  —TAGGED——接口是 VLAN 的一个成员。所有由这个端口传送出来的数据包都是加标记的，携带一个标记因而能够携带 VLAN 或 COS 的信息。

  —UNTAGGED——接口是 VLAN 的一个成员。所有由这个端口传送的数据包是不加标记的，没有携带标记因此也不携带 VLAN 或 COS 的相关信息。注意，一个接口作为一个无标记端口应该至少被分配给一个组。

  —FORBIDDEN——接口从由 GVRP 自动分配 VLAN 中被隐藏。

  —NONE——接口不是 VLAN 中的一个成员，和这个 VLAN 相关联的数据包将不被传送。
- Trunk Member——显示一个端口是否是一个 trunk 的成员。使用 VLAN 静态表页中的最后一个菜单来对选定的 VLAN 添加一个 trunk。

Web——点击 VLAN，VLAN 静态表。从下拉菜单中选择一个 VLAN ID，如果

需要的话修改 VLAN 名称和状态。在端口或 trunk 列标记适当的按钮来选择成员类型。点击 Apply。

VLAN Static Table

VLAN: 2

Name	R&D
Status	☑ Enable

Port	Tagged	Untagged	Forbidden	None	Trunk Member
1	○	◉	○	○	
2	○	○	○	◉	
3	○	○	○	◉	
4	○	○	○	◉	
5	○	○	○	◉	

命令行界面——此例添加了所需的接口。

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport allowed vlan add 2
Switch(config-if)#end
```

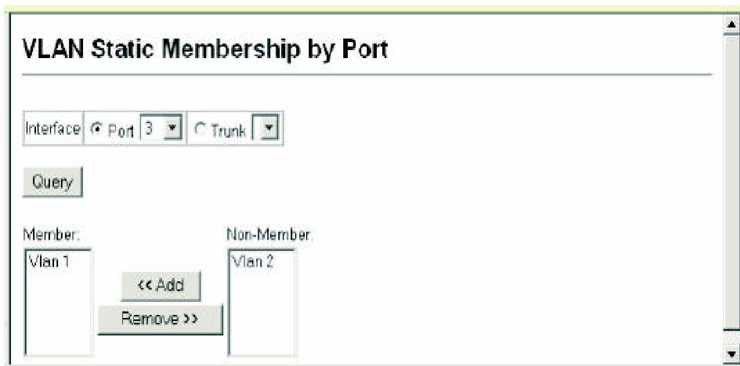
基于静态成员资格添加接口

使用 VLAN 静态成员分配 VLAN 组到已选的界面。添加一个接口到已选的 VLAN 作为标记的成员。

命令属性

- INTERFACE——端口或 trunk 的标识符。
- MEMBER——所选接口是加标记成员的 VLAN。
- NON-MEMBER——所选接口不是加标记成员的 VLAN。

Web——点击 VLAN ，VLAN Static Membership by Port。从下拉对话框中选择一个接口（端口或 trunk）。点击QUERY 显示这个接口的 VLAN 成员信息。选择一个 VLAN ID，然后点击 ADD 以带标记成员的方式添加这个接口，或者点及 REMOVE 以删除这个接口。对每一个接口配置完 VLAN 成员后，点击 Apply。



命令行界面——此例对端口3添加VLAN1作为带标记的端口，从VLAN2除去端口3。

```
Switch(config)#interface ethernet 1/3
Switch(config-if)#switchport allowed vlan add 1
Switch(config-if)#switchport allowed vlan remove 2
Switch(config-if)#
```

为接口配置 VLAN 行为

你可以为特定的接口配置 VLAN 的行为，包括默认的 VLAN 标识符，公认的帧类型，进口过滤，GVRP 状态和 GARP 计时器。

命令的使用

- GVRP——GARP VLAN 注册协议定义了一种方法使得交换机在网络中通过交换 VLAN 信息来达到在接口上自动注册 VLAN 成员的目的。
- GARP——群地址注册协议是 GARP 在桥路局域网中用来为客户服务注册或取消注册客户属性的。GARP 的计时器默认是与介质接入方式和数据速率无关的，这些数值是不应该被修改的，除非你在 GVRP 的注册或取消注册过程中遇到了困难。

命令属性

- 进口过滤——如果进口过滤被激活了，由那些在他们的成员设置中不包括进口端口的 VLAN 发出的数据帧将会在进口端口被丢弃。这将不会影响 VLAN 独立的 BPDU 帧，例如 GVRP 或 STP。
- PVID——分配给在接口处被接受的无标记数据帧的 VLAN ID。如果交换机端口模式被设置为 TRUNK，所有的从无标记端口发出的无标记数据帧都会被加入 PVID。
- 可接受的帧类型——设置端口能够接受所有类型的数据帧，包括无标记和有标记的数据帧，或者只是加标记数据帧。如果只有加标记数据帧被接收，那么交换机只接收帧标签与这个接口被分配的 VLAN 相匹配的数据帧。
- GVRP 状态——对接口激活或是禁止 GVRP。在这个设置生效之前，GVRP 必须在交换机中被全局的激活。当被禁止时，任何的从这个端口被接受的 GVRP 数据包将会被丢弃,而且在其它端口将不会有 GVRP 的注册被广播。
- GARP 加入计时器——传送加入一个 VLAN 组请求和询问的时间间隔。
- GARP 离开计时器——一个端口离开一个 VLAN 组之前等待的时间间隔。这个时间应该被设置为加入时间的两倍以上，这就确保在一个

离开消息和离开所有消息被发出后，这个端口仍然有可能在端口实际离开 VLAN 组之前重新加入。

- GARP 离开所有计时器——向所有 VLAN 组成员发出离开所有消息和端口离开 VLAN 之间的时间间隔。这个时间间隔应该被设置为远远大于离开时间，以最大限度的减少由节点重新加入组而产生的流量。
- trunk 成员——显示一个端口是否是一个 trunk 的成员。使用 VLAN 静态表页中最后一个表来为选定的 VLAN 加一个 trunk。
- 模式——为端口显示 VLAN 的成员模式。

—Access—— 设置端口作为未标记的接口操作。所有的帧未加标记被发送。

—1Q Trunk——指定一个作为 VLAN Trunk 的终点。因为在两台交换机间 Trunk 是直接连接，所以酸口发送未标记的帧，能识别源 VLAN。但是注意属于端口的默认 VLAN 的帧（例：与 PVID 有关）未加标记就被发送。

Web——点击 VLAN，VLAN 端口配置或者 VLAN Trunk 配置。为每一个配置需要的设定，点击 Apply。

VLAN Port Configuration

Ingress Filtering ☑ Enabled

Port	PVID	Acceptable Frame Type	GVRP Status	GARP Join Timer(Centi Seconds)(20-1000)	GARP Leave Timer(Centi Seconds)(60-3000)	GARP LeaveAll Timer(Centi Seconds)(500-18000)	Trunk Member	Mode
1	1	ALL	☐ Enabled	20	60	1000		Access
2	1	ALL	☐ Enabled	20	60	1000		Access
3	2	ALL	☑ Enabled	30	90	2000		1Q Trunk

命令行界面——此例将端口 3 设置为只接受带标记的帧，分配 PVID 3 作为本地 VLAN ID，激活 GVRP，设置 GARP 定时器，然后设置交换机端口模

式为 Trunk。

Switch(config)#interface Ethernet 1/3

Switch(config-if)#switchport acceptable-frame-types tagged

Switch(config-if)#switchport ingress-filtering

Switch(config-if)#switchport native vlan 2

Switch(config-if)#switchport gvrp

Switch(config-if)#garp timer join 30

Switch(config-if)#garp timer leave 90

Switch(config-if)#garp timer leavea11 2000

Switch(config-if)#switchport mode trunk

Switch(config-if)#

配置私有 VLAN

私有 VLAN 允许对默认 VLAN 的修改以提供在 VLAN 端口间的基于端口的安全和分离。下连端口的数据流只能被发送给或从上联端口接收。私有 VLAN 和正常的 VLAN 可以在同一个交换机中同时存在。你可以用私有 VLAN 状态和私有 VLAN 状态链接页来激活或是禁止私有 VLAN 的功能，而且能够将端口配置为上连端口或是下连端口。

请按照以下步骤配置私有 VLAN**：**

1． **使用私有** VLAN **配置菜单指出一个或多个团体** VLAN **和主要** VLAN**。**
2． **使用私有** VLAN **联合菜单映射次要（如团体）**VLAN **到主要** VLAN**。**
3． **使用私有** VLAN **端口配置菜单设置端口类型为混合（例：访问主要** VLAN **中的所有端口）或主机（例：访问团体** VLAN **成员受到限制，引导所有其他数据流通过一个混合端口）。然后将任意混合端口分配到主要** VLAN**，并将任意注意分配到次要** VLAN **（例：团体** VLAN**）。**

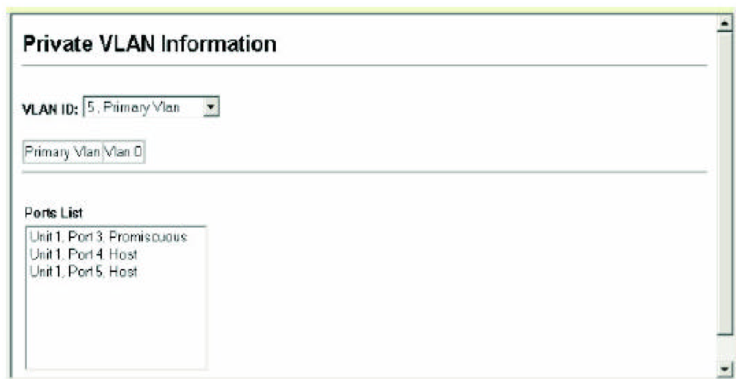
显示当前私有 VLAN

私有 VLAN 信息页显示有关配置到交换机上的私有 VLAN 的信息。包括主要和团体 VLAN 以及相关的接口。

命令属性

- **VLAN ID——已经配置的** VLAN **的** ID（1-4094）。
- **Primary VLAN——和已选的** VLAN **相关的主要** VLAN。
- **Ports List——私有** VLAN **中的端口列表。**

Web ——点击 Private VLAN/Private VLAN Information。**从** VLAN ID **下拉菜单选择想要的端口。**



命令行界面——此例显示了配有主要 VLAN 5 **和次要** VLAN6 **的交换机。当端口** 4、5 **已经被配置为主机端口并与** VLAN6 **关联时，端口** 3 **已经被**

配置为混合端口并映射到 VLAN5。这就是说端口 4、5 的数据流只能通过端口 3。

```
Switch#show vlan private-vlan
Primary   Secondary       Type        Interfaces
--------  -----------  -----------  --------------------
    5                   primary
    5          6        community
    5          7        community
Switch#
```

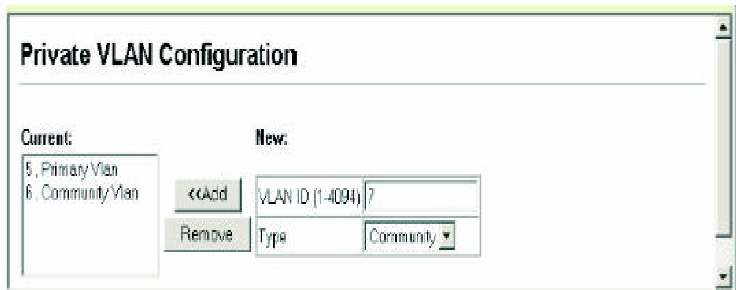
配置私有 VLAN

私有 VLAN 配置页用于创建或除去主要 VLAN 或团体 VLAN。

命令属性

- VLAN ID——已配置的 VLAN 的 ID（1-4094）。
- Type——两种类型的 VLAN。
  - ✧ Primary VLANs——在混合端口间传达数据流，并发送到次要 VLAN 中的共同端口。
  - ✧ Community VLANs——在共同端口间传达数据流，并发送到相关的混合端口。
- Current——显示当前已配置的 VLAN 的列表。

Web——点击私有 VLAN，私有 VLAN 配置，输入 VLAN ID，选择主要或共同类型，然后点击 Add。



命令行界面——此例将 VLAN5 配置为主要 VLAN，端口 6、7 配置为共同 VLAN。

```
Switch(config)#vlan database
Switch(config-vlan)#private-vlan 5 primary
Switch(config-vlan)#private-vlan 6 community
Switch(config-vlan)#private-vlan 7 community
Switch(config-vlan)#
```

与共同 VLAN 建立关联

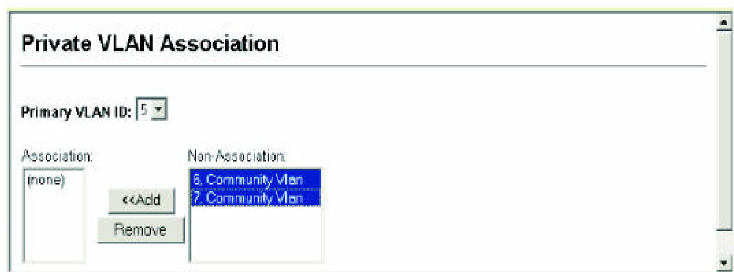
每个共同 VLAN **必须与主要** VLAN **关联。**

命令属性

- **Primary VLAN ID——主要** VLAN **的** ID（1-4094）。
- **Association——已选的主要** VLAN **与共同** VLAN **建立关联。**
- **Non-Association——已选的主要** VLAN **与共同** VLAN **没有建立关联。**

Web——点击私有 VLAN，私有 VLAN 关联，从下拉栏中选择主要 VLAN 或共同类型，在 Non-Association **列表中点亮一个或多个共同 VLAN，点击 ADD**

建立关联。（一个共同 VLAN 只能与一个主要 VLAN 建立关联）



命令行界面——此例将 VLAN 6、7 **和** VLAN 5 **建立关联。**

```
Switch(config)#vlan database
Switch(config-vlan)#private-vlan 5 association 6
Switch(config-vlan)#private-vlan 5 association 7
Switch(config-vlan)#
```

显示私有 VLAN 界面信息

使用私有 VLAN **端口信息和私有** VLAN TRUNK **信息菜单显示与私有** VLAN **相关的界面。**

命令属性

- **Port/Trunk——交换机接口。**
- **PVLAN Port Type——显示私有** VLAN **端口类型。**
- **Primary VLAN——在混合端口间传达数据流，在混合端口和共同端口间传达数据流。**
- **Secondary VLAN——在交换机上，所有的次要** VLAN **是共同** VLAN**，共同** VLAN **在共同端口间传达数据流，从共同端口到指定的混合端口间传达数据流。**

- **Trunk——**Trunk **标识符。**

Web——点击私有 VLAN**，私有** VLAN **端口信息或私有** VLAN TRUNK **信息。**

Private VLAN Port Information

Port	PVLAN Port Type	Primary VLAN	Secondary VLAN	Trunk
1	Normal			
2	Normal			
3	Promiscuous	5		
4	Host		6	
5	Host		6	

命令行界面——此例显示交换机配置了主要 VLAN 5 **和次要** VLAN 6**。当端口** 4、5 **已经被配置为主机端口并与** VLAN6 **关联时，端口** 3 **已经被配置为混合端口并映射到** VLAN5**。这就是说端口** 4、5 **的数据流只能通过端口** 3**。**

```
Switch#show vlan private-vlan
Primary   Secondary     Type        Interfaces
--------  -----------  ----------  ------------------
     5                 primary
     5         6       community
     5         7       community
Switch#
```

配置私有 VLAN 界面

Web——点击私有 VLAN**，私有** VLAN **端口信息或私有** VLAN TRUNK **信息。设置** PVLAN **端口类型加入私有** VLAN**。对于混合端口，设置相关的主要** VLAN**。对于主机端口，设置相关的次要** VLAN**。配置完所有的端口后，点击** Apply**。**

Private VLAN Port Configuration

Port	PVLAN Port Type	Primary VLAN	Secondary VLAN	Trunk
1	Normal	5	6	
2	Normal	5	6	
3	Promiscuous	5	6	
4	Host	5	6	
5	Host	5	6	

命令行界面——此例显示交换机配置了主要 VLAN 5 **和次要** VLAN 6**。当端口** 4、5 **已经被配置为主机端口并与** VLAN6 **关联时，端口** 3 **已经被配置为混合端口并映射到** VLAN5**。这就是说端口** 4、5 **的数据流只能通过端口** 3**。**

```
Switch(config)#interface ethernet 1/3
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#switchport private-vlan mapping 5
Switch(config-if)#exit
Switch(config)#interface ethernet 1/4
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#switchport private-vlan host-association 6
Switch(config-if)#exit
Switch(config)#interface ethernet 1/5
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#switchport private-vlan host-association 6
Switch(config-if)#
```

服务类别的配置

当由于阻塞的原因数据停留在交换机的缓冲器中时，服务类别（CoS）允许你规定什么样的数据包有比较大的优先权。这台交换机对每一个端口支持四个优先权队列，一个端口中优先权比较大的数据包将在优先权较小的数据包之前被传送。你可以对每一个端口设置默认的优先权，然后配置传输帧的优先权标记映射到交换机优先权队列中。

本款交换机对每个端口使用循环作为默认模式。在IEEE 802.1p中定义了多达8个独立的数据流级别。下表显示了默认优先级。

	Queue			
	0	1	2	3
Priority		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

设置队列模式

你能对 4 个服务质量设置队列模式为严格优先级或加权循环（WRR）。默认为 WRR。

命令属性

- WRR——通过分别对1、3、12、48设置队列为0、1、2、3，加权循环共享带宽。
- Strict——严格按照次序服务于外出队列，按照由高到低的优先级发送数据流。

Web——点击Priority，Queue Mode。选择需要的队列模式。点击Apply。



命令行界面——此例使用严格的服务规则设置队列模式。

```
Switch(config)#queue mode strict
Switch(config)#
```

端口 Trunk 配置

你能在设备间创建多个连接。一个端口 Trunk **增加了网段的带宽。并在两个设备间提供容忍错误的连接。你同时能创建多达** 4 **个** Trunk**，每个单一的** Trunk **能包含** 8 **个端口。**

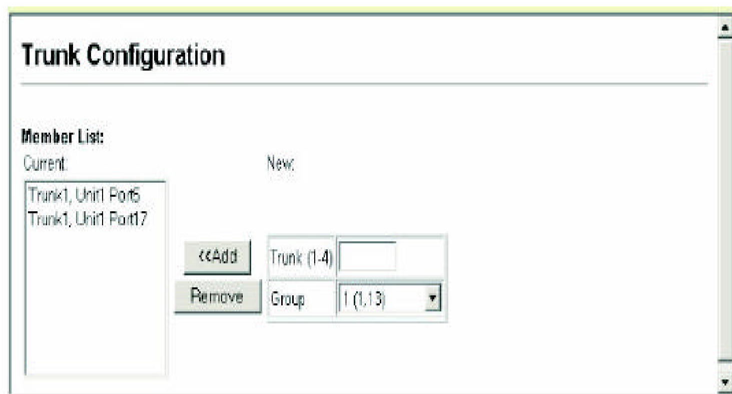
命令属性

- **Current——列出端口当前配置为静态** Trunk **的成员。**
- **New——选择一个预先确定的端口组，添加到这个指定的** Trunk**。**

组的号码	端口
1	1，13
2	1-2，13-14

3	1-4，13-16
4	5，7
5	5-6，17-18
6	5-8，17-20
7	9，21
8	9-10，21-22
9	9-21，21-24
10	25-26

Web——点击 Trunk, Trunk Configuration。**在**Trunk**字段中输入**1-4**个**Trunk ID。**从下拉列中选择任意预先确定的端口组。点击**ADD。**若要除去一个** Trunk，**在**Trunk**字段中输入**Trunk**标识符的类型，点击**Remove。



命令行界面——此例用端口 5 **和** 17 **创建了** Trunk1。**只要连接这些端口到另一台交换机上的两个静态** Trunk **端口，就能形成一个** Trunk。

```
Switch(config)#interface port-channel 1
Switch(config-if)#port-group 1
Switch(config-if)#end
Switch#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type: 100TX
  Mac address: 00-30-F1-68-67-41
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Flow control: Disabled
 Current status:
  Created by: User
  Link status: Down
  Operation speed-duplex: 10half
  Flow control type: None
  Member Ports: Eth1/1, Eth1/13,
Switch#
```

配置 SNMP

SNMP（简单网络管理协议）是一个传输协议，专门用于管理设备或其他网络元素。用 SNMP 管理的设备通常包括交换机，路由器或主机计算机。SNMP 典型的用于配置这些设备，使它们在网络环境中正确的运做，并监控它们来估算性能或侦测潜在的问题。

交换机包含一个随机携带的SNMP代理，它时刻监控硬件状态和通过端口的数据流。网络管理站能使用诸如AccView或HP OpenView等软件访问此信息。对SNMP代理的访问权利由团体字符串控制。为了和交换机进行通信，管理站必须首先递交一个有效的团体字符串用于认证。配置团体字符串的选项和有关的陷阱功能下面有详细描述。

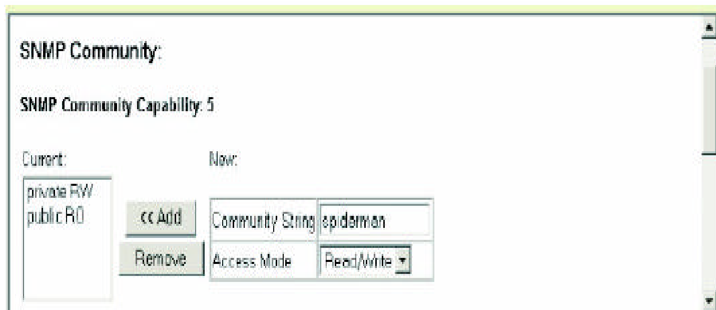
设置团体访问字符串

你可以配置多达 5 个经管理访问认证的团体字符串。所有用于 IP 陷阱管理器的团体字符串应该列在这个表中，你应该考虑除去默认字符串。

命令属性

- **SNMP Community Capability**——显示交换机支持多达 5 个团体字符串。
- **Community String**——团体字符串的功能就像密码，并允许访问 SNMP 协议。
  默认字符串："共同"（只读），"私有"（读/写）
  范围：1-32 个字符，区分大小写
- **Access Mode**
  - ✧ **Read-Only**——指定只读访问。认证的管理站点只能找回 MIB 对象。
  - ✧ **Read/Write**——指定读写访问。认证的管理站点能找回并更改 MIB 对象。

Web——点击 SNMP, SNMP 配置。添加新的团体字符串点击，从访问模式下拉菜单选择访问权利，然后 Apply。



命令行界面——下例用读/写访问添加了字符串“spiderman”。

```
Switch(config)#snmp-server community spiderman rw
Switch(config)#
```

指定陷阱管理器和陷阱类型

命令的使用

- **你能通过** WEB **接口激活或禁用认证信息。**
- **你能通过命令行界面激活或禁用认证信息或**link-up-down**信息。**

命令属性

- **Trap Manager Capability——显示交换机支持多达** 5 **个陷阱管理器。**
- **Trap Manager IP Address——主机的因特网地址。**
- **Trap Manager Community String——像密码的团体字符串和通知操作一起发送。虽然你可以在陷阱管理器表中设置这个字符串，但建议您也在** SNMP **协议表中定义这个字符串。**
  范围：1-32 **个字符，区分大小写。**

- **Enable Authentication Traps——在** SNMP **访问认证过程中，无论一个有效的团体字符串是否被递交，都会发行一个陷阱信息。**

Web——点击 SNMP, SNMP Configuration。**对每个陷阱管理器填写** IP **地址和团体字符串，如有需要，请标记激活认证陷阱。然后点击** ADD。

Trap Managers:

Trap Manager Capability: 5

Current: (none)

New:

<< Add | Remove

Trap Manager IP address	10.1.19.23
Trap Manager Community String	batman

Enable Authentication Traps: ☑

命令行界面——下例添加了陷阱管理器并激活了认证陷阱。

```
Switch(config)#snmp-server host 10.1.19.23 bitway
Switch(config)#snmp-server enable traps authentication
```

显示端口统计表

Web——点击 Statistics, Port Statistics。**选择需要的接口并点击**Query。**你也能使用**Refresh**按钮更新界面。**

Port Statistics

Interface ◉ Port 1 ○ Trunk 1

Query

Interface Statistics:

Received Octets	140335	Received Unicast Packets	1335
Received Multicast Packets	0	Received Broadcast Packets	17
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	1695197
Transmit Unicast Packets	1624	Transmit Multicast Packets	923
Transmit Broadcast Packets	2	Transmit Discarded Packets	0

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	147563	Collisions	0
Received Frames	0	64 Bytes Frames	1120
Broadcast Frames	17	65-127 Bytes Frames	157
Multicast Frames	0	128-255 Bytes Frames	5
CRC/Alignment Errors	0	256-511 Bytes Frames	138
Undersize Frames	0	512-1023 Bytes Frames	6
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

命令行界面——下例显示了端口 1 的统计表。

```
Switch#show interfaces counters ethernet 1/5
Ethernet 1/ 5
 Iftable stats:
  Octets input: 0, Octets output: 64
  Unicast input: 0, Unicast output: 0
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 1
  Broadcast input: 0, Broadcast output: 0
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 0, Packets: 0
  Broadcast pkts: 0, Multi-cast pkts: 0
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 0, Packet size 65 to 127 octets: 0
  Packet size 128 to 255 octets: 0, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Switch#
```

速率限制配置

此功能允许网络管理者能控制发送或接收数据流的最大速率。在速率限制范围内的数据流被发送，而数据包超过数据流的量，就会被丢弃。

速率限制能应用于单独的端口或 TRUNK。当一个接口被配置了此特性，数据流速率将被硬件监控，来检验是否符合。不符合的数据流被丢弃，符合的数据流原封不动的被转发。

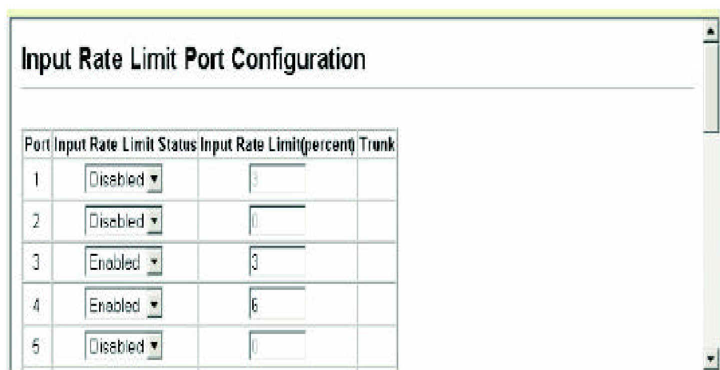
命令属性

- **Port/Trunk——交换机接口。**

- **Rate Limit Status——激活或禁用速率限制。**
- **Rate Limit (Percent)——设置速率限制为预先确定的带宽百分比。**

选项	百分比（基于端口类型）		
	10 Mbps	**100Mbps**	**100 Mbps**
3	312K	3.12M	31.2M
6	625K	6.25M	62.5M
9	938K	9.38M	93.8M
12	1.25M	12.5M	125M
20	2M	20M	200M
40	4M	40M	400M
60	6M	60M	600M
80	8M	80M	800M

Web——点击 Rate Limit, Input/Output Rate Limit Port/Trunk Configuration。**对所需的接口激活速率限制状态，设置速率限制为先前表格中的一项，点击**APPLY。



命令行界面——此例设置通过端口3**的输入输出数据流的速率限制约为**3%**（例：对于**100Mbps**连接，限制速率为**3.12Mbps**），通过端口**4**的数据流的速率限制约为**4-6%**（例：对于**100Mbps**连接，限制速率为**6.25Mbps**）。**

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#rate-limit input percent 3
Switch(config-if)#rate-limit output percent 3
Switch(config-if)#exit
```

第三章 命令行界面

本章讲述如何使用命令行界面（CLI）。

使用命令行界面

访问 CLI

当通过直接联接交换机到服务器的控制端口或是通过 Telnet 接入到交换机的管理接口上时，我们可以通过在提示符下输入命令关键字和参数来控制交换机。使用交换机的命令行界面与在 UNIX 系统下输入命令是非常相似的。

控制台联接

通过控制台端口接入交换机，请按以下步骤操作：

1. 在控制台提示下，输入用户名和密码。默认的用户名是 admin，口令为空；和 guest，密码是 guest。
   - 当管理员的用户名和密码被输入后，命令行界面显示“Switch#”提示并且进入特权接入模式。
   - 当普通用户名和密码被输入后，命令行界面显示“Switch>”提示并且进入普通接入模式。
2. 输入必须的命令来完成你想要的任务。
3. 当完成后，用“quit”或“exit”命令退出。

当通过控制台端口连接到系统后，接入屏幕显示：

```
User Access Verification

Username: admin
Password:

      CLI session with the BitStream BS3224TM+ is opened.
      To end the CLI session, enter [Exit].

Switch#
```

Telnet 联接

Telnet 是在 IP 传输协议之上运行的。在这种环境下，你的控制站和任何网络中你想要控制的设备都必须有有效的 IP 地址。有效的 IP 地址是由四个 0 到 255 的数字组成的，有点号分离。每一个地址是由网络部分和主机部分组成的。例如，分配给这台交换机的 IP 地址是 10.1.0.1，由网络部分（10.1.0）和主机部分（1）组成。

通过 Telnet 会话访问交换机，你必须首先为交换机设置 IP 地址，如果你正从不同的 IP 子网管理交换机，你还需设置默认网关。例：

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.5 255.255.255.0
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.254
Switch(config)#
```

如果你的共同网络被联接到了你办公室外的另外一个网络或者是互联网上，你就需要申请一个注册过的网络。但是，如果你被联接到了一个隔离的网络，你就可以用任何一个与你的网段匹配的 IP 地址。

当你设置完你的交换机的 IP 地址之后，你就可以按照以下步骤打开 Telnet 会话。

1． 从远端的主机，输入 Telnet 命令和你所要登录的设备的 IP 地址。

2． 根据提示，输入用户名和密码。命令行界面将会对管理员显示“Vty-0#”提示符以显示你现在所在的模式是特权接入模式，或者“Vty-0>”以显示模式是普通用户模式。
3． 输入必要的命令已完成你的任务。
4． 当完成上述的步骤后，使用“quit”或是“exit”命令退出。

当输入 Telnet 命令后，接入屏幕会显示：

```
Username: admin
Password:

CLI session with the host is opened.
To end the CLI session, enter [Exit].

Vty-0#
```

注意：你可以通过 Telnet 对设备打开四个会话。

输入命令

这一节描述怎样输入 CLI 命令。

关键字和主题

一个命令行界面命令是由一系列的关键字和主题组成的。关键字规定了一个命令，主题规定了配置的参数。例如在命令“ show interfaces status ethernet 1/5”中，show interfaces和status就是关键字，ethernet是规定端口类型的主题，1/5规定了单位/端口。

输入命令如下：

- 如输入一个简单的命令，输入命令的关键字。
- 如输入一个复杂的命令，以需要的顺序输入没一个命令。例如，为

了激活特权命令模式，并且显示开始的配置，输入：

```
Switch>enable
Password:
Switch#show startup-config
```

- 为了输入需要参数的命令，在输入命令关键字后输入需要的参数。例如，为管理员设置一个用户名和密码，输入：

```
Switch(config)#username admin password 0 bitway
```

最小缩写

命令行界面能够接受可以唯一区别一个命令的最小字符的组合。例如，命令“configure”可以输入“config.”。如果输入不明确，系统将会提示进一步的输入。

命令完成

如果你用 Tab 键来终止命令的输入，命令行界面将会输出根据你已经输入的字符而可能输入的命令。例如，输入 log，再按下 Tab 键，系统将会打印出命令“logging”

得到关于命令的帮助

你可以输入 help 命令显示帮助。你也可以用“？”字符列出关键字和参数来显示命令的语法。

显示命令

如果你在命令提示下输入了“？”符号，系统将会根据当前的命令级别和配置级别来显示第一级的关键字。你也可以显示关于一个特定的命令的一系列的关键字。例如，命令“show ? ”显示了一列可能显示的命令

```
Switch#?
Exec commands:
  clear       Reset functions
  configure   Enter configuration mode
  copy        Copy from one file to another
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  dot1x       Configure 802.1x
  exit        Exit from privilege EXEC mode
  help        Description of the interactive help system
  ip          Internet protocol
  ping        Send echo messages
  quit        Exit a CLI session
  reload      Halt and perform a warm restart
  show        Show information
  whichboot   Determine boot files
Switch#
```

命令“show interface?”将会显示以下的信息：

```
Switch>show interface ?
  counters     Information of interfaces counters
  status       Information of interfaces status
  switchport   Information of interfaces switchport
```

部分关键字的查询

如果你用一个询问标记终止了部分关键字，与最初字母符合的关键字将会被显示出来。例如输入“s?”，将会显示以 s 开头的关键字。

```
Switch#show s?
snmp            spanning-tree   startup-config  system
Switch#show s
```

否定命令的作用

对于许多配置命令你可以输入前缀“no”来取消一个命令的作用或者是将配置重新设置为默认值。例如 logging 命令会将系统信息传送到主机服务器，为了禁止传送，指定 no logging 命令。这个指南将会描述所有可应用的命令的否定作用。

使用命令历史纪录

命令行界面包含一个曾经输入过的命令的的历史纪录，你可以使用上箭头键在命令历史纪录中搜寻。任何在历史纪录中显示的命令可以被重新执行，或者是修改后再执行。
使用 show history 命令显示最近的更长的执行命令列表。

理解命令模式

这个命令设置被分为 EXEC 和 CONFIGURATION 级别。EXEC 命令一般来说会显示系统状态信息或是清除统计表计数器。另一方面，CONFIGURATION 命令会修改界面参数或激活某些交换功能。这些级别又被进一步的被分为不同的模式，可用的命令取决于你选的模式，你总是能输入问号?来显示在当前模式下你可用的命令。命令级别和相关模式在下表中显示：

Class	Mode
Exec	Normal Privileged
Configuration*	Global Interface Line VLAN

*你必须在特权 EXEC 模式下访问任何配置模式。

EXEC 命令

当你用用户名 GUEST 在交换机上打开一个新的控制线程，系统进入普通 EXEC 命令模式。在这种模式下一部分命令可以被执行，你在特权 EXEC 命令模式下可以获得全部命令。为了进入特权命令模式，输入用户名 ADMIN，或者输入 ENABLE 命令。在普通 EXEC 命令模式下提示符是 SWITCH〉，而在特权 EXEC 命令模式下提示符是 SWITCH#。

输入下列命令和密码进入特权 EXEC 命令模式：

```
User Access Verification

Username: admin
Password:

      CLI session with the BitStream BS3224TM+ is opened.
      To end the CLI session, enter [Exit].

Switch#
```

```
Username: guest
Password:

      CLI session with the BitStream BS3224TM+ is opened.
      To end the CLI session, enter [Exit].

Switch>enable
Password:
Switch#
```

配置命令

配置命令是特权级别的命令，用来修改交换机的设置。这些命令只修改交换机运行时的配置并且在交换机重新启动后是不会被保存的。使用copy running-config startup-config命令来在非易失性存储介质上保存运行设置。

这些配置命令被组织成三种模式：

- **全局配置——这些命令修改系统级别的设置，并且包含如hostname和snmp-server community这样的命令。**
- **接口配置——这些命令修改端口配置，例如speed-duplex和negotiation这样的命令。**
- **行配置——这些命令修改控制台端口的配置，例如parity和databits这样的命令。**

若要进入全局配置模式，在特权EXEC模式下输入CONFIGURE命令，系统提示将会变成SWITCH#，这将使你能访问所有全居配置命令。

```
Switch#configure
Switch(config)#
```

若要进入其他模式，在配置提示下输入以下一个命令。使用额exit或end

回到特权EXEC模式。

Mode	Command	Prompt
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)#
Line	line {console | vty}	Console(config-line)#
VLAN	vlan database	Console(config-vlan)

例如，你可以使用以下命令输入界面配置模式，然后返回特权EXEC模式。

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#exit
Switch(config)#
```

命令行处理

命令是不区分大小写的。你可以缩写任何的命令和参数只要这足以将它和别的可以获得的命令和参数区分开来，你可以使用TAB键来完成未完的命令部分，或者输入部分命令和一个“？”来显示可以获得的一些命令列。你也可以使用下列编辑键来进行命令行处理：

按键	功能
Ctrl-A	切换指针到命令行启动
Ctrl-B	切换指针到一个字符的左边
Ctrl-E	切换指针到命令行的尾部
Ctrl-F	切换指针到一个字符的右边
Ctrl-P	显示上一个命令
Ctrl-U	删除整行
Ctrl-W	删除最后键入的单词
删除键或退格键	输入命令时，擦去错误

命令组

系统命令能够被分解为功能组，如下所示：

Command Group	Description
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI
Flash/File	Manages code image or switch configuration files
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information
Authentication	Configures authentication for logon access using local or RADIUS methods
SNMP	Activates authentication failure traps; configures community access strings, and trap managers
Line	Sets communication parameters for the serial port and Telnet, including baud rate and console time-out.
IP	Configures the IP address and gateway for management access, displays the default gateway, or pings a specified device
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs
Rate Limiting	Sets the maximum rate for traffic transmitted or received on an interface
Address Table	Configures the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time
Spanning Tree	Configures Spanning Tree settings for the switch
VLAN	Configures VLAN settings, defines port membership for VLAN groups
PVLAN	Enables or configures private VLANs
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB
Priority	Sets port priority for untagged frames, also sets the service weight for each priority queue based on strict priority or Weighted Round Robin
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port
Port Trunking	Statically groups multiple ports into a single logical trunk

注意：下表中的接入模式是以缩写的形式来表示的：

NE(普通 EXEC)

PE(特权 EXEC)

GC（全局配置）

IC（接口配置）

LC（行配置）

VC（VLAN 数据库配置）

常规命令

命令	功能	模式
Enable	激活特权模式	NE
Disable	从特权模式返回常规模式	PE
Configure	激活全局配置模式	PE
Show history	显示命令历史缓冲	NE，PE
Reload	重启系统	PE
End	返回特权 EXEC 模式	GC，IC，LC，VC
Exit	返回先前的配置模式或退出命令行界面	any
Quit	退出命令行界面对话	NE，PE
Help	显示如何使用帮助	any
?	对命令完成显示选项	any

enable

用这个命令激活特权 EXEC 模式，在特权模式下，可以获得附加的命令，某些命令显示附加的信息。

语法

enable[*level*]

level——连接进设备的特权级别。

这个设备有两个预定义的特权级别：0：普通 EXEC，15：特权 EXEC。进入级别 15 就以特权模式接入了设备。

默认的设置

级别 15

命令模式

普通 EXEC

命令的利用

- 如果从普通 EXEC 命令模式转换到特权 EXEC 命令模式需要默认的密码 super。
- 字符#被加在了系统提示符后边表示当前系统是工作在特权接入模式下的。
- 你值需要使用级别 15。为级别 0 设置密码是没有作用的。
- 你不能用命令 enable password 设置空密码，你必须输入一个密码以进入特权 EXEC 模式。

例：

```
Switch>enable
Password:
Switch#
```

相关的命令

DISABLE

ENABLE PASSWORD

disable

用这个命令从特权 EXEC 模式返回到普通 EXEC 模式。在普通接入模式下，你只能显示交换机或者 VDSL/以太网统计表的基本信息。为了能够获得所

有的命令，你必须进入特权模式。

默认的设置

无

命令模式

特权 EXEC

命令的使用

符号〉被连结到了系统提示符后边显示当前系统是工作在普通接入模式下的。

例：

```
Switch#disable
Switch>
```

相关的命令

ENABLE

configure

使用此命令来激活全局配置模式。你必须输入此模式更改任何交换机的设置。你必须输入全局配置模式的优先级来激活其它一些配置模式，包括接口配置，行配置和 VLAN 数据库配置。

默认的设置

无

命令模式

特权 EXEC

例：

```
Switch#configure
Switch(config)#
```

相关命令

END

show history

使用此命令显示命令历史缓存。

默认的设置

无

命令模式

普通 EXEC，特权 EXEC

命令的使用

历史缓存的大小固定为 10 个执行命令和 10 个配置命令。

例：

此例中，历史命令列出命令历史缓存的目录。

```
Switch#show history
Exection command history:
 6 enable
 5 disable
 4 enable
 3 show history
 2 conf
 1 show history

Configuration command history:
 3 interface vlan 1
 2 exit
 1 exit

Switch#
```

当你在特权 EXEC 或普通 EXEC 模式下时，符号！重复在执行命令历史缓存中的命令。在这个例子中，!2 重复执行了在命令历史缓存中的第二个命令。

```
Switch#!2
Switch#conf
Switch(config)#
```

reload

使用这个命令来重启系统。

注意：系统重新启动时，它总是会执行开机自检。由命令 copy running-config startup-config，它也会保留所有保存在非易失性存储介质中的配置信息。

默认设置

无

命令模式

特权 EXEC

命令的使用

此命令重新设置整个系统。

例:

这个例子显示了怎样重启交换机：

```
Switch#reload
System will be restarted, continue <y/n>?
```

end

用此命令重新返回特权 EXEC 模式。

默认设置

无

命令模式

全局配置，界面配置，行配置，VLAN 数据库配置。

例:

这个例子显示了怎样从接口配置模式返回到特权 EXEC 模式：

```
Switch(config-if)#end
Switch#
```

exit

用这个命令返回到先前的配置模式或是退出当前的配置模式。

默认设置

无

命令模式

任何

例:

这个例子显示了怎样从全局配置模式返回到特权 EXEC 模式，然后退出命令行界面会话。

```
Switch(config)#
Switch(config)#exit
Switch#exit
% CLI exit session
```

quit

用这个命令退出配置程序。

默认设置

无

命令模式

普通 EXEC，特权 EXEC

命令的使用

QUIT 和 EXIT 命令都能退出配置程序。

例：

这个例子显示了如何退出一个命令行界面会话：

```
Switch#quit
% CLI exit session
```

FLASH/FILE 命令

这些命令用来管理系统代码或配置文件：

命令	功能	模式
Copy	将代码映像或交换机配置复制到闪存或 TFTP 服务器；	PE

	或从闪存或 TFTP 服务器复制代码映像或交换机配置	
Delete	删除一个文件或代码映像	PE
Dir	显示闪存中的文件列	PE
Whichboot	显示导入文件	PE
Boot system	指定用于启动系统的文件或映像	GC

copy

用这个命令在交换机的闪存和 TFTP 服务器之间拷贝代码映像或是配置文件。当你向 TFTP 服务器上的一个文件保存系统代码或配置设定时，这个文件可以在以后被交换机下载以恢复默认设置。文件传送的成功依赖于 TFTP 服务器的易接进性和网络连接的质量。

语法

copy *file* {file | running-config | startup-config | tftp}

copy running-config {file | startup-config | tftp}

copy startup-config {file | running-config | tftp}

copy tftp {file | running-config | startup-config}

- *file*——允许你向或是从一个文件拷贝的关键字。
- running-config——允许你向或是从现有的运行配置拷贝的关键字。
- startup-config——用于系统初始化的配置。
- tftp——允许你从或是向一个 TFTP 服务器拷贝的关键字。

默认的设置

无

命令的模式

特权 EXEC

命令的使用

- 完成拷贝命令所需的数据的系统提示。
- 目的配置文件的名称，不应该包含斜线，文件名称的开头字母不应该为点号。
- 用户定义的配置文件的最大数目是由所能获得闪存空间所决定的。
- 你可以把文件 Factory_Default_Config.cfg 作为目的文件从出厂默认配置文件拷贝，但是你不能把这个文件作为目的文件。
- 为了替换启动配置，你必须使用 startup-config 作为目的文件。
- BOOT ROM 不能作为源文件或是目的文件从 TFTP 服务器上下载。你必须遵循导入时候显示的控制信息来下载 BOOT ROM 映像。

例：

下例显示了如何上传配置设定到 TFTP 服务器上的一个文件：

```
 Switch#copy file tftp
 Switchfile type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

 Switch#
```

下例显示了如何拷贝运行配置到启动文件中：

```
Switch#copy running-config startup-config
Startup configuration file name [test]: startup
Write to FLASH Programming.
Write to FLASH finish.
Success.

Switch#
```

下例显示了如何下载一个配置文件：

```
Switch#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Switch#
```

delete

用这个命令删除一个文件或映像。

语法

delete ***filename***

filename——配置文件或是映像文件的名字。

默认设置

无

命令模式

特权 EXEC

命令的使用

- 如果文件类型是 BOOT ROM 或是用来系统启动的，则不能被删除。

- 不能删除“Factory_Default_Config.cfg”文件。

例

此例显示了如何从闪存中删除 test 配置文件：

```
Switch#delete test
Switch#
```

相关的命令

dir

dir

使用这个命令显示闪存中的一系列文件。

语法

dir [boot-rom | config | opcode [:*filename*]]

显示的文件或映像的类型包括：

- **boot-rom**——BOOT ROM 映像文件
- **config**——交换机配置文件
- **opcode**——文件或映像的名字。如果这个文件存在担包含错误，这个文件中的信息不能被显示。
- *filename*——所显示文件的文件名。如果文件存在但有错，此文件中的信息不能显示。

默认设置

无

命令模式

特权 EXEC

命令的使用

- 如果你不带任何参数输入 dir 命令，系统将显示所有文件。
- 文件信息如下所示：

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

例:

下边的例子说明如何显示所有文件信息：

```
Switch#dir
                        file name      file type startup size (byte)
 -------------------------------- -------------- ------- -----------
                             diag Boot-Rom image       Y       78592
                          runtime Operation Code       Y      764672
       Factory_Default_Config.cfg    Config File       Y        2536
                          startup    Config File       N        3367
 -------------------------------------------------------------------
                                          Total free space:   933888
Switch#
```

whichboot

用这个文件显示哪些文件被导入。

默认设置

无

命令模式

特权 EXEC

例:

这个例子显示了由命令 whichboot 显示的信息。

```
Switch#whichboot
                           file name      file type startup size (byte)
 -------------------------------- -------------- ------- -----------
                                diag Boot-Rom image       Y       78592
                             runtime Operation Code       Y      764672
       Factory_Default_Config.cfg    Config File       Y        2536
Switch#
```

boot system

用这个命令指定用于启动系统的文件或映像。

语法

boot system {boot-rom| config | opcode}: ***filename***

按默认设置的文件或映像的类型包括：

- boot-rom——BOOT ROM
- config——配置文件
- opcode——运行操作代码

冒号不能省略。

Filename——配置文件或映像的名称。

默认设置

无

命令模式

全局配置

命令的使用

- 在指定完文件后，需要冒号。
- 如果文件中包含错误，它不能被指定为默认文件。

例：

```
Switch(config)#boot system config:startup
Switch(config)#
```

相关命令

dir

whichboot

系统管理命令

系统管理命令使用来控制系统的接入，密码，用户名，浏览器配置选项和显示或配置一系列的其他系统信息。

hostname

用这个命令来指定或修改这台设备的主机名称。使用 no 的形式来恢复默认的主机名称。

语法

hostname name

no hostname

name——主机的名字。(最大长度：255 字符)

默认设置

无

命令模式

全局配置

例：

```
Switch(config)#hostname bitway
Switch(config)#
```

username

这个命令使得登录时需要用户名认证,使用 no 的形式来删除一个用户名。

语法

username *name* {access-level *level* | nopassword | {0 | 7} password *password*}

no username *name*

- name——用户的名字
- （最大长度：8 个字符；用户最大数目：5）
- access-level *level*——规定用户的级别。
- 这个设备有两个预定义的特权级别：
  0：普通 EXEC，15：特权 EXEC
- nopassword——这个用户登录不需要密码。
- {0 | 7}——0 意味着无格式密码，7 意味着加密密码。
- password *password*——对这个用户的认证密码。

默认设置

- 默认的接入模式是特权 EXEC.
- 在普通 EXEC 模式下密码是 guest，在特权模式下密码是空。

用户名和密码的出厂默认设置是：

username	access-level	password
guest admin	0 15	guest 空

命令模式

全局配置

命令的使用

加密密码是为了当读取系统启动时的配置文件或从 TFTP 服务器下载配置文件时，兼容原先的密码设置（例：无格式文本或加密）。

例:

这个例子显示了怎样为一个用户设置访问级别和密码：

```
Switch(config)#username alan access-level 15
Switch(config)#username alan password 0 leaf
Switch(config)#
```

Enable password

连结进系统之后，你应该为客户和管理员设置密码，应该把他们放在安全的地方。用这个激活密码的命令来控制从普通 EXEC 模式转到特权 EXEC 模式，使用 NO 方式来重新设置默认密码。

语法

enable password [level *level*] {0 | 7} *password*

no enable password [level *level*]

level *level*——密码所应用的级别。

- 对于这个命令只有级别 15 是有效的。
- {0 | 7}——0 意味着无格式密码，7 意味着加密密码。
- *password*——这个特权级别的密码。

默认设置

- 默认级别是 15
- 默认的密码是 super

命令模式

全局配置

命令的使用

- 你不能设置空密码。用 ENABLE 命令输入密码更改普通 EXEC 命令模式为特权 EXEC 模式。
- 加密密码是为了当读取系统启动时的配置文件或从 TFTP 服务器下载配置文件时,兼容原先的密码设置(例 :无格式文本或加密)。无须手动配置加密密码。

实例

```
Switch(config)#enable password level 15 0 admin
Switch(config)#
```

相关命令

ENABLE

Ip http port

用这个命令指定被网络浏览器接口所使用的 TCP 端口数，使用 NO 形式来使用默认的端口。

语法

ip http port *port-number*

no ip http port

***port-number*——被网络浏览器使用的 TCP 端口。（范围：1-65535）**

默认设置

80

命令模式

全局配置

例:

```
Switch(config)#ip http port 769
Switch(config)#
```

相关命令

IP HTTP SERVER

Ip http server

这个命令允许设备能够从浏览器上被监控或配置，用 NO 的形式禁用这个功能。

语法

ip http server

no ip http server

默认设置

激活

命令模式

全局配置

例:

```
Switch(config)#ip http server
Switch(config)#
```

相关命令

IP HTTP PORT

show startup-config

使用这个命令来显示用来启动系统的存储在非易失性存储介质上的配置文件。

默认设置

无

命令模式

特权 EXEC

命令的使用

- 结合使用此命令和show running-config命令比较运行内存中的信息和固定内存中的信息。
- 此命令显示关键命令模式的设置。每个模式组由“！”分割，包括配置模式命令和相关命令。此命令显示以下信息：

—用户

—SNMP团体字符串

—VLAN数据库（VLAN ID，名字和状态）

—每个界面的VLAN配置设置

—默认VLAN的IP地址

—控制台端口和TELNET的任意配置设置

例：

```
switch#show startup-config
building startup-config, please wait.....
!
username admin access-level 15
username admin password 0 admin
!
username guest access-level 0
username guest password 0 guest
!
enable password level 15 0 super
!
snmp community public ro
snmp community private rw
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1

   .
   .
   .

interface ethernet 1/26
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
!
interface vlan 1
 ip address 10.1.0.1 255.255.255.0
!
!
line switch
!
!line vty


end
switch#
```

相关命令

SHOW RUNNING-CONFIG

Show running-config

使用这个命令显示当前正在使用的配置信息。

默认设置

无

命令模式

特权 EXEC

命令的使用

- **结合使用此命令和show startup-config命令比较运行内存中的信息和固定内存中的信息。**
- **此命令显示关键命令模式的设置。每个模式组由“！”分割，包括配置模式命令和相关命令。此命令显示以下信息：**

—用户

—SNMP团体字符串

—VLAN数据库（VLAN ID，名字和状态）

—每个界面的VLAN配置设置

—默认VLAN的IP地址

—控制台端口和 TELNET 的任意配置设置

例：

```
 switch#show running-config
building running-config, please wait.....
!
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active.
!
!
interface ethernet 1/1
 switchport allowed vlan add 1
 switchport native vlan 1
 switchport mode access
.
.
.
!
interface vlan 1
 ip address 10.1.0.1 255.255.255.0
!
!
!
!
!
!
line switch
!
!
line vty
!
!
!
end
 switch#
```

相关命令

show startup-config

show system

用这个命令显示系统信息。

默认设置

无

命令模式

普通 EXEC，特权 EXEC

例：

```
Switch#show system
System description: Intelligent Management Switch
System OID string: 1.3.6.1.4.1.13157.1.2.1.14
System information
 System Up time: 0 days, 0 hours, 34 minutes, and 50.12 seconds
 System Name              : bitway
 System Location          : [NONE]
 System Contact           : [NONE]
 MAC address              : 00-30-F1-68-67-40
 Web server               : enable
 Web server port          : 769
 POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test......................PASS
Flash Memory Checksum Test..............PASS
CPU Self Test...........................PASS
MPC850 clock Timer and Interrupt TEST...PASS
WatchDog Timer and Interrupt Test.......PASS
DRAM Test...............................PASS
ACD Chip Test...........................PASS
Switch Driver Initialization............PASS
I2C R/W Test............................PASS
Switch Internal Loopback Test ..........PASS
------------------- DONE --------------------
Switch#
```

show users

显示所有的活动着的控制和远程登录线程，包括用户名，空闲时间和 IP 地址以及远程登录客户。

默认设置

无

命令模式

普通 EXEC，特权 EXEC

命令的使用

用于执行此命令的会话由“ * ”显示，在行（例：会话）索引编码旁。

例:

```
Switch#show users
 Username accounts:
  Username Privilege
  -------- ---------
     admin        15
     guest         0

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
* 0   console    admin           0:00:00

Switch#
```

show version

用这个命令显示系统的硬件和软件版本号。

默认设置

无

命令模式

普通 EXEC，特权 EXEC

命令的使用

- **Serial Number ——主板的系列号**
- **Hardware Version——主板的硬件版本号**
- **Number of Ports ——交换机上的端口数**
- **Module Type ——安装在交换机中的模块类型**

- **Main Power Status ——交换机的电源状态**

例:

```
Switch#show version
Unit1
 Serial number          :
 Hardware version       :
 Module A type          :1000Base-LX-SC SMF
 Module B type          :1000Base-SX-SC MMF
 Number of ports        :26
 Main power status      :up
Agent(master)
 Unit id                :1
 Loader version         :1.0.0.3
 Boot rom version       :1.0.0.3
 Operation code version :1.0.3.3
Switch#
```

认证命令

远程认证拨如用户服务（RADIUS）是一个使用运行着 RADIUS 软件的中心服务器来控制网络中接入识别 RADIUS 的设备的系统。一个 RADIUS 服务器包含一个由很多用户名和密码组成的数据库，每一个用户或组都由一个对应的特权级别，这个数据库需要用控制端口，远程登录或 Web 方式对交换机进行管理接入。

authentication login

使用这个命令来定义登录认证的方式和优先级别。使用 NO 的方式来恢复默认的设置。

语法

authentication login {[**local**] [**radius**]}

no authentication login

- **radius**——只使用 RADIUS 服务器密码。
- **local**——只使用本地密码。

默认设置

无

命令模式

全局配置

例:

```
Switch(config)#authentication login radius
Switch(config)#
```

相关命令

USERNAME——设置本地用户名和密码。

radius-server host

使用这个命令来指定 RADIUS 服务器。用 NO 的形式来恢复默认设置。

语法

radius-server host *host_ip_address*

no radius-server host

host_ip_address - IP address of server.

默认设置

无

命令模式

全局配置

例:

```
Switch(config)#radius-server host 192.168.1.25
Switch(config)#
```

radius-server port

用这个命令来设置 RADIUS 服务器网络端口，使用 NO 的形式来恢复默认设置。

语法

radius-server port *port_number*

no radius-server port

port_number——用来给认证消息的 RADIUS 服务器 UDP 端口。(范围：1-65535)

默认设置

1812

命令模式

全局配置

例:

```
Switch(config)#radius-server port 181
Switch(config)#
```

radius-server key

用这个命令来设置 RADIUS 加密，使用 NO 的形式来恢复默认的设置。

语法

radius-server key *key_string*

no radius-server key

key_string——用来鉴别用户登录的加密字符。字符串中请勿使用空格。（最大长度：20 个字符）

默认设置

无

命令模式

全局配置

例:

```
Switch(config)#radius-server key alan
Switch(config)#
```

radius-server retransmit

用这个命令设置重试的次数，使用 NO 的方式来恢复默认值。

语法

radius-server retransmit ***number_of_retries***

no radius-server retransmit

number_of_retries——交换机通过 RADIUS 服务器试图登录认证的次数。（范围：1-30）

默认设置

无

命令模式

全局模式

例:

```
Switch(config)#radius-server retransmit 5
Switch(config)#
```

radius-server timeout

用这个命令来设置向 RADIUS 服务器传送认证请求的时间间隔，使用 NO 方式来恢复默认的设置。

语法

radius-server timeout *number_of_seconds*

no radius-server timeout

number_of_seconds——交换机重新发送请求前等待应答的秒数。（范围：1-65535）

默认设置

5

命令模式

全局配置

例:

```
Switch(config)#radius-server timeout 10
Switch(config)#
```

show radius-server

用这个命令来显示 RADIUS 服务器当前的设置。

默认设置

无

命令模式

特权 EXEC

例:

```
Switch#show radius-server
Remote radius server configuration:
 Server IP address: 192.168.1.25
 Communication key with radius server: alan
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10
Switch#
```

SNMP 命令

使用 SNMP 从管理站控制对交换机的访问，和发送给陷阱管理器的错误类型。

snmp-server community

用这个命令来定义对简单网络管理协议的接入团体字符，使用 NO 的形式来删除现有的设置。

语法

snmp-server community *string* [ro|rw]

no snmp-server community *string*

- ***string*——象密码一样的团体字符并且允许对 SNMP 协议的接入。**
- **ro——规定只读方式接入。认证的管理站只能回收 MIB 对象。**
- **rw——规定可读可写模式接入。认证的管理站既能回收又能修改 MIB 对象。**

默认设置

- **PUBLIC——只读方式接入。认证的管理站只能回收 MIB 对象。**

- PRIVATE——可读可写方式接入。认证的管理站既能回收又能修改 MIB 对象。

命令模式

全局配置

命令的使用

你输入的第一个 SNMP-SERVER COMMUNITY 命令激活 SNMP，NO SNMP-SERVER COMMUNITY 命令禁止所有版本的 SNMP 协议。

例：

```
Switch(config)#snmp-server community alan rw
Switch(config)#
```

snmp-server contact

使用这个命令来设置系统的联系字符串，使用 NO 的方式来删除系统的联系信息。

语法

snmp-server contact *string*

no snmp-server contact

string——描述系统联系信息的字符串。（最大长度：255 个字符）

默认设置

无

命令属性

全局配置

例：

```
Switch(config)#snmp-server contact leaf
Switch(config)#
```

相关命令

snmp-server location

snmp-server location

使用这个命令设置系统的位置字符串，使用 NO 的形式来删除系统的位置字符串。

语法

snmp-server location *text*

no snmp-server location

***text*——描述系统位置的字符串。（最大长度：255 个字符）**

默认设置

无

命令模式

全局配置

例：

```
Switch(config)#snmp-server location bitway
Switch(config)#
```

相关命令

SNMP-SERVER CONTACT

snmp-server host

用这个命令指定一个简单网络管理协议通告操作的接收者，使用 NO 的形

式来删除已指定的主机。

语法

snmp-server host *host-addr community-string*

no snmp-server host *host-addr*

- *host-addr*——主机的名字或因特网地址，
- *community-string*——同认证操作一起发出的像密码的团体字符。尽管你可以用 snmp-server host 命令设置这个字符串，但是我们推荐你使用 snmp-server community 命令。

默认设置

无

命令模式

全局配置

命令的使用

如果你没有输入 snmp-server host 命令，没有通告被发送。为了配置这台交换发送 SNMP 通告，你必须输入至少一个 snmp-server host 命令。为了激活多个主机，你必须为每一个主机发出一个 snmp-server host 命令。snmp-server host 命令是与 snmp-server enable traps 命令一起使用的，用 snmp-server enable traps 命令来指定哪一个 SNMP 的通告被全局发送。对于一台接收通告的主机，至少一个 snmp-server enable traps 命令和 snmp-server host 命令在这台主机上被激活。但是，一些通告类型是不能被 snmp-server enable traps 命令来控制的。例如，一些通告类型是始终被激活的。

例：

```
Switch(config)#snmp-server host 10.1.19.23 alan
Switch(config)#
```

相关命令

snmp-server enable traps

snmp-server enable traps

使用这个命令来激活这个设备使他发送简单网络管理协议陷阱或通告，使用 NO 的形式来禁止 SNMP 通告。

语法

snmp-server enable traps [authentication | link-up-down]

no snmp-server enable traps [authentication | link-up-down]

- **authentication——发送一个认证失败陷阱的关键字。**
- **link-up-down——发送连上或断开陷阱的关键字。**

注意：link-up-down 陷阱只能通过命令行界面来激活或是禁止。

默认设置

发送所有陷阱

命令模式

全局配置

命令的使用

如果你没有输入一个 snmp-server enable traps 命令，没有被这个命令控制的通告被发出。为了配置这台设备发出 SNMP 通告，你必须输入至少一个 snmp-server enable traps 命令。如果你不带关键字的输入这个命令，所有的通告类型都会被激活，如果你带关键字的输入这个命令，只由于这个关键字相关的通告类型被激活。

命令 snmp-server enable traps 是与 snmp-server host 一同使用的。使用 snmp-server host 命令来指定哪台或是哪些主机接收 SNMP 通告，为了发送这个通告，你必须至少配置一个 snmp-server host

命令。在这个命令中使用的通告类型有一个相关联的 MIB 对象，这使得他们能够被全局的激活或是禁止。不是所有的通告类型都有通告激活 MIB 对象，所以其中的一些是不能被 snmp-server enable traps 命令来控制的。

例：

```
Switch(config)#snmp-server enable traps link-up-down
Switch(config)#
```

相关命令

SNMP-SERVER HOST

Show snmp

使用这个命令来检查 SNMP 通讯的状态。

默认设置

无

命令模式

普通 EXEC，特权 EXEC

命令的使用

这个命令提供有关团体访问字符串的信息，SNMP输入输出协议数据单位的计数器信息，SNMP日志是否被**snmp-server enable traps**命令激活。

例:

```
Switch#show snmp
System Contact: leaf
System Location: bitway

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. alan, and the privilege is read-write
   2. private, and the privilege is read-write
   3. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
   0 Trap PDUs

SNMP logging: enabled
    Logging to 10.1.19.23
Switch#
```

行命令

通过连接 VT100 兼容设备到服务器的串口，你能访问随机携带的配置程序。这些命令用于设置串口或 TELNET（例：虚拟终端）的通信参数。

line

使用这些命令来识别特定的行进行配置，并处理并发行配置命令。

语法

line {console | vty}

- **console**——控制台终端行
- **vty**——远程控制台访问的虚拟终端

默认设置

无

命令模式

全局配置

命令的使用

TELNET 被认为是虚拟终端连接，界面显示为“ VTY ”，如 show users。但是连续的通信参数（例：数据位）不影响 TELNET 连接。

例：

输入控制台行模式，输入以下命令：

```
Switch(config)#line console
Switch(config-line)#
```

相关命令

show line

show users

login

用此命令在登录时来激活密码检查。使用 NO 禁用密码检查，这样没有密码也能连接。

语法

login [local]

no login

local——选择本地密码检查。认证基于username命令指定的用户名。

默认设置

本地注册

命令模式

行配置

例：

```
Switch(config-line)#login local
Switch(config-line)#
```

相关命令

username

password

password

使用此命令对行指定密码。使用 NO 的形式除去密码。

语法

password {**0** | **7**} *password*

no password

- {**0** | **7**}——0指无格式密码，7指加密密码
- password——指定行密码的字符串。

  （最大长度：8个字符，32位加密，区分大小写）

默认设置

无

命令模式

行配置

例：

```
Switch(config-line)#password 0 bitway
Switch(config-line)#
```

相关命令

login

password-thresh

exec-timeout

使用此命令设置时间间隔。使用 NO 形式禁用 timeout 功能。

语法

exec-timeout *seconds*

no exec-timeout

默认设置

CLI: 无

Telnet: 10分钟

命令模式

行配置

命令的使用

- 如果用户输入在超时时间间隔内被侦测，会话则持续打开；否则会话终止。
- 此命令适用于本地控制台和TELNET连接。
- TELNET超时不能禁用。

例：

设置超时为2分钟，输入此命令：

```
Switch(config-line)#exec-timeout 120
Switch(config-line)#
```

password-thresh

使用此命令来设置密码入侵域值，限制失败登录的次数。使用 NO 形式除去域值。

语法

password-thresh ***threshold***

no password-thresh

threshold——允许密码的次数

（范围：1-120，无域值）

默认设置

三次

命令模式

行配置

例：

设置密码域值为5次，输入次命令：

```
Switch(config-line)#password-thresh 5
Switch(config-line)#
```

相关命令

silent-time

silent-time

用此命令设置失败登录后无法访问管理控制台的时间的长度。使用 NO 形式除去沉默时间的值。

语法

silent-time ***seconds***

no silent-time

默认设置

无

命令模式

行配置

例：

设置默认时间为0秒，输入此命令：

```
Switch(config-line)#silent-time 60
Switch(config-line)#
```

相关命令

password-thresh

databits

使用此命令设置每个字符数据位的数目，字符由控制台口生成。使用 NO 形式恢复默认值。

语法

databits {7 | 8}

no databits

- **7——每字符7个数据位**
- **8——每字符8个数据位**

默认设置

每字符8个数据位

命令模式

行配置

例：

若要指定7个数据位，如下输入：

```
Switch(config-line)#databits 8
Switch(config-line)#
```

相关命令

parity

parity

使用此命令来定义奇偶位的产生。使用 NO 的形式恢复默认设置。

语法

parity {none | even | odd}

no parity

- **none——无奇偶**
- **even——偶数位**
- **odd——奇数位**

默认设置

无

命令模式

行配置

命令的使用

设备提供的传输协议如终端和MODEM 通常需要特定的奇偶位设置。

例：

若要指定无奇偶，输入如下命令：

```
Switch(config-line)#parity none
Switch(config-line)#
```

speed

使用此命令设置终端行的波特率。此命令同时设置传输和接收速度。使用 NO 的形式恢复默认设置。

语法

speed ***bps***

no speed

bps**——每秒波特率**

（选项：9600, 57600, 38400, 19200, 115200 bps）

默认设置

9600bps

命令模式

行配置

例：

指定57600bps，**输入如下命令：**

```
Switch(config-line)#speed 9600
Switch(config-line)#
```

stopbits

使用此命令设置停止位（以每字节被发送）的数目。使用 NO 的形式恢复默认设置。

语法

stopbits {1 | 2}

- 1——1**个停止位**
- 2——2**个停止位**

默认设置

1 **个停止位**

命令模式

行配置

例：

若要指定2**个停止位，输入如下命令：**

```
Switch(config-line)#stopbits 1
Switch(config-line)#
```

show line

使用此命令显示终端行参数。

语法

show line [console | vty]

- **console** ——控制台终端行
- **vty** ——远程控制台访问的的虚拟终端

默认设置

显示所有的行

命令模式

普通EXEC，特权EXEC

例：

若要显示所有的行，输入如下命令：

```
Switch#show line
 Console configuration:
  Password threshold: 5 times
  Interactive timeout: 120 sec
  Silent time: 60 sec
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

 Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 600 sec
Switch#
```

IP 命令

默认情况下，交换机没有分配 IP 地址。你必须手动配置一个新的地址管理网络中的交换机。你也可能需要在交换机与另一个网段中的管理站之间建立一个默认网关。

ip address

用这个命令给交换机设置 IP 地址，使用 NO 的形式恢复默认 IP 地址。

语法

ip address {*ip-address netmask* | **bootp** | **dhcp**}

no ip address

- *ip-address*——IP 地址
- *netmask*——相关的 IP 子网的网络掩码。这个子网识别用来路由到特定子网的主机地址位。
- **bootp**——从 BOOTP 获得 IP 地址。
- **dhcp**——从 DHCP 获得地址。

默认设置

IP 地址：0.0.0.0

网络掩码：255.0.0.0

命令模式

接口配置（VLAN）

命令的使用

- 你必须为这台交换机分配 IP 地址，使它能够获得对网络的管理权利。你可以手动的配置一个 IP 地址，或者让设备通过 DHCP 或 BOOTP

获得一个 IP 地址。有效的 IP 地址由四个 0 到 255 的数字组成，由点隔开。此外的 IP 地址都不会被配置程序接受。

- 如果你选择 BOOTP 或 DHCP 选项,在 BOOTP 或 DHCP 响应被接收之前，IP 地址只是被激活而没有行使功能。这台设备为了学习它的 IP 地址而周期性的广播请求。
- 你可以通过输入 ip dhcp restart 命令或重新启动交换机来开始广播 BOOTP 或 DHCP 请求。

注意：只有一个 VLAN 接口能够被分配给一个 IP 地址，这就定义了管理 VLAN，通过这个 VLAN 你可以获得对这台设备的管理接入。如果你分配一个 IP 地址给其它的 VLAN，这个 IP 地址将越过原来的 IP 地址而成为新的管理 VLAN。

例:

在下边的例子中，设备被分配了 VLAN 1 中的一个地址。

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.5 255.255.255.0
Switch(config-if)#
```

相关命令

ip dhcp restart

ip dhcp restart

使用这个命令来提交一个 BOOTP 或 DHCP 客户请求。

默认设置

无

命令模式

特权 EXEC

命令的使用

- 如果可行，DHCP 要求服务器重新分配一个 IP 地址给客户。
- 如果 BOOTP 或 DHCP 服务器被转移到了不同的域中，分配给客户的地址的网络部分将会基于新的域。

例:

在下边的例子中，设备将会被重新分配相同的地址：

```
Switch(config)#interface vlan 1
Switch(config-if)#ip add dhcp
Switch(config-if)#end
Switch#ip dhcp restart
Switch#show ip interface
 IP address and netmask: 0.0.0.0 255.0.0.0 on VLAN 1,
 and address mode: DHCP.
Switch#
```

相关命令

ip address

ip default-gateway

使用这个命令在这台设备和另外一个网段中的管理站之间建立一个静态路由。使用 NO 的形式来删除静态路由。

语法

ip default-gateway *gateway*

no ip default-gateway

gateway——默认网关的 IP 地址

默认设置

没有静态路由被建立。

命令模式

全局配置

命令的使用

如果管理站位于一个不同的 IP 网段时，必须定义网关。

例:

下边的例子为这台设备定义了一个默认网关：

```
Switch(config)#ip default-gateway 10.1.0.254
```

相关命令

show ip redirects

show ip interface

使用这个命令来显示一个 IP 接口的设置。

默认设置

所有接口

命令模式

特权 EXEC

命令的使用

这台交换机只能被分配一个地址，这个地址用来管理这台交换机。

例:

```
Switch#show ip interface
 IP address and netmask: 192.168.1.5 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Switch#
```

相关命令

show ip redirects

show ip redirects

使用这个命令来显示交换机默认网关的配置。

默认设置

无

命令模式

特权 EXEC

例:

```
Switch#show ip redirects
ip default gateway  0.0.0.0
```

相关命令

ip default-gateway

ping

使用这个命令向网络中的另外一个节点发送 ICMP 回波请求包。

语法

ping *host* [**count** *count*][**size** *size*]

- *host*——IP 地址或是主机的 IP 名称
- *count*——发送包的个数
- *size*——每一个包的大小

  实际的发送的包的大小比规定的包的大小多出 8 个字节，因为交换机加入了主题信息。

默认设置

这个命令对主机没有默认设置

命令模式

普通 EXEC，特权 EXEC

命令的使用

- 使用这个命令来确定网络中的另外一个点是否可以达到。
- 下边是一些 PING 命令的结果：
    - 普通回应——普通回应发生在 1 到 10 秒钟，依赖于网络的流量。
    - 目的没有响应——如果主机没有响应，no answer from host 信息将会被显示。
    - 目的不能到达——目的的网关显示这个目的是不能被到达的。
    - 网络或主机不能获得——网关在路由表中找不到响应的入口。
- 按 Esc 键停止 PING。

例:

```
Switch#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Switch#
```

相关命令

interface

接口命令

这些命令使用为以太网端口，集成连接或 VLAN 显示或设置通讯参数的。

interface

这个命令用来配置一个接口类型并且输入接口配置模式。使用 NO 的形式除去 TRUNK。

语法

interface *interface*

no interface port-channel *channel-id*

interface

- **以太网** ***unit/port***

  —*unit*——这是设备 1

  —*port*——端口号

- **端口通道** ***channel-id***
- **VLAN** ***vlan-id***

默认设置

无

命令模式

全局配置

例：

若要指定端口 25，输入相应命令：

```
Switch(config)#interface ethernet 1/25
Switch(config-if)#
```

description

使用这个命令对接口添加描述，使用 NO 的形式删除描述。

语法

description ***string***

no description

string——注释或描述。帮助你记住这个接口连接了何种设备。

（范围：1-64 个字符）

默认设置

无

命令模式

接口配置

例：

下边的例子为以太网端口 25 添加了描述：

```
Switch(config)#interface ethernet 1/25
Switch(config-if)#description bitway
Switch(config-if)#
```

speed-duplex

这个命令用于自适应被禁止后，对已给的接口配置速度和双工模式，使用 NO 的形式来恢复默认设置。

语法

speed-duplex {1000full | 100full | 100half | 10full | 10half}

no speed-duplex

- **1000full**——强制 1000Mbps 全双工操作
- **100full**——强制 100Mbps 全双工操作
- **100half**——强制 100Mbps 半双工操作
- **10full**——强制 10Mbps 全双工操作

◆ 10half——强制 10Mbps 半双工操作

默认设置

- 自适应默认为激活
- 当自动流通被禁止时，默认的速度双工模式对 100BASE-TX 端口是 100half，100BASE-FX 端口是 100full，Gigabit 以太网端口是 1000full。

命令模式

接口配置

命令的使用

- 为了使用 speed-duplex 命令对速度和双工模式进行强制操作，我们需要对选定的接口用 no negotiation 命令来禁止自适应。
- 当使用negotiation命令激活自适应时，最佳设置设置将由 capabilities命令决定。在自适应下设置速度和双工模式，必须在性能列中指定所需的模式。

例：

下边的例子将端口 5 配置为 100Mbps，半双工模式：

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#speed-duplex 100half
Switch(config-if)#no negotiation
Switch(config-if)#
```

相关命令

negotiation

capabilities

negotiation

使用这个命令对已给接口激活自适应，使用 NO 的方式来禁止自适应。

语法

negotiation

no negotiation

默认设置

激活

命令模式

接口配置

命令的使用

- **当自适应被激活，交换机将基于 capabilities 命令对连接调整最佳的设置。当自适应禁用，你必须用 speed-duplex 和 flowcontrol 命令手动指定连接属性。**
- **如果自动流通被禁止了，给 RJ-45 端口的 auto-MDI/MDI-X 管脚信号配置也会被禁止。**

例：

这个例子使用自适应配置了端口 11。

```
Switch(config)#interface ethernet 1/11
Switch(config-if)#negotiation
Switch(config-if)#
```

相关命令

capabilities

speed-duplex

negotiation

capabilities

使用这个命令在自适应时广告接口的端口容量，使用 NO（带参数）的方式删除一个已广播的容量，或是不带参数的方式来恢复默认设置。

语法

capabilities {1000full | 100full | 100half | 10full | 10half | flowcontrol |symmetric}

no port-capabilities [1000full | 100full | 100half | 10full | 10half |flowcontrol | symmetric]

- 1000full——支持 1000Mbps 全双工操作
- 100full——支持 100Mbps 全双工操作
- 100half——支持 100Mbps 半双工操作
- 10full——支持 10Mbps 全双工操作
- 10half——支持 10Mbps 半双工操作
- flowcontrol——支持流控
- symmetric——当指定时，端口发送和接收暂停帧；未指定时，端口将执行自适应，对非均衡暂停帧决定发送器和接受器。

默认设置

- 快速以太网：10half，10full，100half，100full
- Gigabit 以太网：1000full

命令模式

接口配置

例：

下边的例子将以太网端口 5 的性能设置为 100half,100full 和流控。

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#capabilities 100half
Switch(config-if)#capabilities 100full
Switch(config-if)#capabilities flowcontrol
Switch(config-if)#
```

相关命令

negotiation

speed-duplex

flowcontrol

flowcontrol

使用这个命令激活流控。使用 NO 的形式来禁止流控。

语法

flowcontrol

no flowcontrol

默认设置

激活流控

命令模式

接口配置

命令的使用

- **流控能够减少由终端机和交换机直接连接时由于缓冲器饱和引起的数据帧丢失，当激活后，背压用于来半双工操作，IEEE802.3X 用于全双工操作。**

- **若要强制打开或关闭流控(用 flowcontrol 或 no flowcontrol 命令)，使用 no negotiation 命令禁用选定端口的自适应功能。**
- **当使用 negotiation 命令激活自适应时，最佳的设置将由 capabilities 命令决定。若要激活流控，端口性能列中必须包括“**flowcontrol**”。**
- **对于连接到集线器的端口请避免使用流控。除非它确实需要解决一个问题。否则背压干扰信号可能降低连接了集线器的网段的性能。**

例：

下边的例子激活端口 5 的流控功能：

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#flowcontrol
Switch(config-if)#no negotiation
Switch(config-if)#
```

相关命令

negotiation

capabilities

shutdown

使用这个命令来禁用一个接口,是用 NO 的形式来重新启用被禁用的接口。

语法

shutdown

no shutdown

默认设置

所有接口是被激活的。

命令模式

接口配置

命令的使用

这个命令允许你由于不正常的行为（例：过多冲突）而禁用一个端口，并且允许在问题解决之后重新激活这个端口。你也可以出于安全考虑禁用端口。

例：

这个例子禁用了端口 5：

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#shutdown
Switch(config-if)#
```

switch broadcast percent

使用这个命令来配置广播风暴控制。使用 NO 形式来禁用广播风暴控制。

语法

switchport broadcast percent *level*

no switchport broadcast

level—域值级别作为带宽百分比。（范围：6%-20%）

默认设置

激活所有端口

带宽的 6%

命令模式

接口配置（以太网）

命令的使用

- 当广播数据流超过了指定的域值，超过域值的数据包就会被丢弃。
- 这个命令能对已选的接口激活或禁用广播风暴控制。

例：

下例显示了如何在端口 3 上配置广播风暴控制为 20%。

```
Switch(config)#interface ethernet 1/3
Switch(config-if)#switchport broadcast percent 20
Switch(config-if)#
```

clear counters

使用此命令清除接口统计表。

语法

clear counters *interface*

interface

- **ethernet** unit/port

  —*unit*——这是设备1

  —*port*——端口数目

- **port-channel** *channel-id*（范围：1-4）

默认设置

无

命令模式

特权EXEC

例

下例清除了以太网端口5的统计表。

```
Switch#clear counters ethernet 1/5
Switch#
```

show interfaces status

使用这个命令显示一个接口的状态。

语法

show interfaces status *interface*

interface

- 以太网 *unit/port*
  - —*unit*——设备 1
  - —*port*——端口号
- 端口通道 *channel-id*（范围：1-4）
- VLAN *vlan-id*（范围：1-4094）

默认设置

无

命令模式

普通 EXEC，特权 EXEC

命令的使用

如果没有指定接口，则显示所有接口的信息。

例：

```
Switch#show interfaces status ethernet 1/3
Information of Eth 1/3
 Basic information:
  Port type: 100TX
  Mac address: 00-30-F1-68-67-43
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full,
  Broadcast storm: Enabled
  Broadcast storm limit: 20 percent
  Flow control: Disabled
 Current status:
  Link status: Down
  Operation speed-duplex: 10half
  Flow control type: None
Switch#
```

show interfaces counters

使用这个命令显示一个接口的统计表。

语法

show interfaces counters ***interface***

interface*——以太网 *unit/port

- ***unit*——设备 1**
- ***port*——端口号**

默认设置

无

命令模式

普通 EXEC，特权 EXEC

命令的使用

如果没有指定接口，则显示所有接口的信息。

例：

```
Switch#show interfaces counters ethernet 1/7
Ethernet 1/ 7
 Iftable stats:
  Octets input: 0, Octets output: 0
  Unicast input: 0, Unicast output: 0
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 0
  Broadcast input: 0, Broadcast output: 0
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 0, Packets: 0
  Broadcast pkts: 0, Multi-cast pkts: 0
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 0, Packet size 65 to 127 octets: 0
  Packet size 128 to 255 octets: 0, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Switch#
```

show interfaces switchport

使用这个命令显示高级接口配置设定。

语法

show interfaces switchport [*interface*]

interface

- ◆ 以太网 *unit*/*port*

—*unit*——设备 1

—*port*——端口号

◆ 端口通道 *channel-id*

默认设置

显示所有端口

命令模式

普通 EXEC，特权 EXEC

例：

这个例子显示了设为主机模式时，端口 2 配置设定：

```
Switch#show interfaces switchport ethernet 1/2
Information of Eth 1/2
 Broadcast threshold: Enabled, 6 percent
 Ingress rate limit: Disabled
 Egress rate limit: Disabled
 VLAN membership mode: Access
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
 Private-vlan mode: NONE
 Private-vlan host-association: NONE
 Private-vlan mapping: NONE
Switch#
```

此例显示了设为混合模式时，端口 3 的配置设定。

```
Switch#show interfaces switchport ethernet 1/3
Information of Eth 1/3
 Broadcast threshold: Enabled, 20 percent
 Ingress rate limit: Disabled
 Egress rate limit: Disabled
 VLAN membership mode: Access
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    1(u),
 Forbidden Vlan:
 Private-vlan mode: NONE
 Private-vlan host-association: NONE
 Private-vlan mapping: NONE
Switch#
```

速率限制命令

这个功能允许管理者限制端口发送和接收数据的最大速率。速率限制也可以被应用到整个网络中，速率在限制之内的数据被传输，超过了限制将会被丢弃。

rate-limit

使用这个命令设置速率限制。使用 NO 的形式来恢复默认数值。

语法

rate-limit {**input** | **input** } **percent** *percent*

no rate-limit input

- **input——设置流入数据流的速率限制**
- **output——设置流出数据流的速率限制**
- *percent***——设置速率限制为预先确定的带宽百分比**

选项	百分比（基于端口类型）		
	10 Mbps	100Mbps	100 Mbps
3	312K	3.12M	31.2M
6	625K	6.25M	62.5M
9	938K	9.38M	93.8M
12	1.25M	12.5M	125M
20	2M	20M	200M
40	4M	40M	400M
60	6M	60M	600M
80	8M	80M	800M

默认设置

无

命令模式

接口配置

例：

此例设置了端口 2 的流入数据流和输出数据流的速率限制为：当以 10Mbps 操作时为 312K；当 100Mbps 操作时为 3.12Mbps。

```
Switch(config)#interface ethernet 1/2
Switch(config-if)#rate-limit input percent 3
Switch(config-if)#rate-limit output percent 3
Switch(config-if)#
```

地址表命令

这些命令使用来配置地址表以过滤指定的地址，显示现有的条目，清空表格或设置老化时间。

mac-address-table static

使用这个命令映射静态地址到目的端口,使用 NO 的形式来删除一个地址。

语法

mac-address-table static *mac-address* {*interface* | **discard**} [*action*]

no mac-address-table static *mac-address* [**discard**]

- *mac-address*——MAC**地址**
- *interface*
  - ◆ **ethernet** *unit/port*

    —*unit*——**这是设备**1

    —*port*——**端口数目**
  - ◆ **port-channel** *channel-id* (**范围：**1-4)
- **discard——丢弃所有匹配目的地址的数据包**
- *action*

  —delete-on-reset——分配持续到交换机重启

  —permanent——分配是永久的

默认设置

没有静态地址被定义，默认的模式是永久性的。

命令模式

全局配置

命令的使用

主机设备的静态地址能够分配给特定 VLAN 中的一个指定端口。使用这个命令将静态地址添加到 MAC 地址表中，静态地址有下列特性：

- ■ **当已给的接口连接断掉后，静态地址不能从地址表中删除。**

- 静态地址是分配给接口的而且不能被删除。当在界面上可以看见一个静态地址，这个地址将被忽略且不能被写入地址表。
- 只有静态地址用此命令的 NO 形式，才能在另一个端口被学习到静态地址表。

例：

```
 Switch(config)#mac-address-table static 00-e0-29-94-34-de ethernet 1/1
vlan 1 delete-on-reset
 Switch(config)#
```

clear mac-address-table dynamic

使用此命令从转发数据库删除任意键值。

默认设置

无

命令模式

特权 EXEC

例

```
Switch#clear mac-address-table dynamic
Switch#
```

show mac-address-table

使用这个命令在桥路转发数据库中察看条目的级别。

语法

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*]

[**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address*——MAC地址
- *mask*——地址中忽略的位
- *interface*
  - **ethernet** *unit*/*port*

    —*unit*——这是设备1

    —*port*——端口数目
  - **port-channel** *channel-id* (范围：1-4)
- *vlan-id*——VLAN ID（范围：1-4094）
- **sort**——由地址、VLAN或接口进行分类

默认设置

无

命令模式

特权 EXEC

命令的使用

- MAC 地址表包含与每个接口相关的 MAC 地址。注意类型字段应该包括下列类型：

  —可学习的——动态地址条目

  —永久的——静态条目

  —Delete-on-reset——当系统重新启动后被删除的条目
- 地址条目的最大数目是 8191

例：

```
Switch#show mac-address-table
 Interface Mac Address        Type
 --------- ----------------- ---------------------
Switch#
```

mac-address-table aging-time

使用此命令对地址表中的条目设置老化时间。使用 NO 的形式恢复默认老化时间。

语法

mac-address-table aging-time *seconds*

no mac-address-table aging-time

默认设置

300 **秒**

命令模式

全局配置

命令的使用

老化时间用于动态的老化掉可学习的转发信息。

例

```
Switch(config)#mac-address-table aging-time 100
Switch(config)#
```

show mac-address-table aging-time

使用此命令显示地址表中的条目设置老化时间。

默认设置

无

命令模式

特权EXEC

例

```
Switch#show mac-address-table aging-time
 Aging time: 100 sec.
Switch#
```

生成树命令

此部分包括对交换机全局配置 STA（生成树算法）的命令，以及为已选接口配置 STA 的命令。

spanning-tree

使用这个命令为交换机激活生成数算法，使用 NO 的形式禁用 STA。

语法

spanning-tree

no spanning-tree

默认设置

生成树被激活

命令模式

全局配置

命令的使用

生成数算法能够检测出并禁用网络环路，并且在交换机、桥路或路由器间建立备份连接。这就允许这台交换机与网络中的其它桥路设备相通讯以确保网络中的任何两台工作站之间只存在一条路由，并

且当主要连接断掉之后，它会自动启用备用连接。

例：

这个例子显示了怎样激活一台交换机上的生成数算法：

```
Switch(config)#spanning-tree
Switch(config)#
```

spanning-tree forward-time

使用这个命令为交换机全局配置生成树转发时间，使用 NO 的形式恢复默认设置。

语法

spanning-tree forward-time *seconds*

no spanning-tree **forward-time**

- *seconds*——时间以秒计（范围：4-30 秒）
- 最小的值取 4 和[(max-age / 2) + 1]的较大值

默认设置

15 秒

命令模式

全局配置

命令的使用

这个命令设置了根设备改变状态（例：侦听-学习-转发）前等待的最大时间。这个延迟是需要的，因为每台设备在转发数据帧之前都必须接收有关拓扑是否改变的信息。另外，每个端口需要时间去侦听可能导致堵塞状态的冲突信息；否则，可能产生临时数据环路。

例：

```
Switch(config)#spanning-tree forward-time 20
Switch(config)#
```

spanning-tree hello-time

使用这个命令来为交换机全局配置生成树桥路问候时间，使用 NO 的方式恢复默认设置。

语法

spanning-tree hello-time *time*

no spanning-tree hello-time

- ***seconds*——时间以秒计（范围：1-10 秒）**
- **最大的值取** 10 **和**[(max-age / 2) + 1]**的较小值**

默认设置

2 **秒**

命令模式

全局配置

命令的使用

这个命令设置根节点设备发送配置信息的时间间隔。

例：

```
Switch(config)#spanning-tree hello-time 5
Switch(config)#
```

spanning-tree max-age

使用这个命令为交换机全局配置生成树路桥的最大寿命，使用 NO 的形式恢复为默认值。

语法

spanning-tree max-age *seconds*

no spanning-tree max-age

- *seconds*——时间以秒计（范围：6-40 秒）
- 最小值是 6 与[2 x (hello-time + 1)]之间的较大者。
- 最大值是 40 与[2 x (forward-time - 1)]之间的较小者。

默认设置

20 秒

命令模式

全局配置

命令的使用

这个命令设置了一台设备在尝试去配置之间由于没有受到配置信息而能等待的最大时间，在规则的时间间隔内所有的设备端口（除了指定的端口）应该收到配置信息。任何老化掉 STA 信息的端口会变为指定的端口。如果它是根端口，则从设备端口选出一个新的根端口。

例：

```
Switch(config)#spanning-tree max-age 20
Switch(config)#
```

spanning-tree priority

使用这个命令为交换机全局配置生成树优先级，用 NO 的形式来恢复默认值。

语法

spanning-tree priority *priority*

no spanning-tree priority

- *priority*——桥路的优先级（范围：0-65535）

默认数值

32768

命令模式

全局配置

命令的使用

这个命令用于选择根节点设备，根端口和指定端口。有着最高优先级的设备成为 STA 根设备。但是，如果所有的设备有着同样的优先级，那么 MAC 地址最小的设备将成为根设备。

例：

```
Switch(config)#spanning-tree priority 40000
Switch(config)#
```

spanning-tree cost

用这个命令为特定的接口配置生成数路径成本。使用 NO 的形式恢复默认值。

语法

spanning-tree cost *cost*

no spanning-tree cost

cost——对端口的路径成本（范围：1-65535）

推荐的范围是：

-以太网：50-600

-快速以太网：10-60

-千兆以太网：3-10

默认设置

- 以太网——半双工：100；全双工：95；trunk：90
- 快速以太网——半双工：19；全双工：18；trunk：15
- 千兆以太网——全双工：4；trunk：3

命令模式

接口配置

命令的使用

- 这个命令被生成数算法用来决定设备间的最佳路径，因此，更小的数值应该分配给端口以获得更快的速度，高一些的数值对应慢一些的速度。
- 路径成本优先于端口优先级

例：

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#spanning-tree cost 50
Switch(config-if)#
```

spanning-tree port-priority

使用这个命令为指定接口配置优先级，使用 NO 的形式恢复默认值。

语法

spanning-tree port-priority *priority*

no spanning-tree port-priority

- ◆ *priority*——端口的优先级（范围：0-255）

默认设置

128

命令模式

接口配置

命令的使用

- 这个命令定义了在一个生成树算法中一个端口的优先级。如果一个交换机上的所有端口的路径成本都是相同的，有着最高优先级的端口就会被配置为生成树中的一个激活的连结。
- 如果由不止一个端口被分配给了最高优先级，有着最低数字标识符的端口将被激活。

例：

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#spanning-tree port-priority 0
Switch(config-if)#
```

相关命令

spanning-tree cost

spanning-tree portfast

使用这个命令设置接口为快速转发，使用 NO 的形式禁用快速转发。

语法

spanning-tree portfast

no spanning-tree portfast

默认设置

禁用

命令模式

接口配置

命令的使用

- 这个命令用对选定的端口激活或禁用快速生成树模式。在这种模式下，端口跳过堵塞，侦听和学习状态而直接转发。
- 因为终端节点不能引起转发环路，它们能以更快的速度通过生成树状态改变。快速转发对于终端接点工作站和服务器能够达到更快的集中时间，并且也能克服其他的 STA 超时问题。

例：

```
Switch(config)#interface ethernet 1/5
Switch(config-if)#spanning-tree portfast
Switch(config-if)#
```

show spanning-tree

使用这个命令来显示生成树的配置信息。

语法

show spanning-tree [*interface*]

interface

- 以太网 *unit/port*
  - -*unit*——这是设备 1
  - -*port*——端口数目
- port-channel——信道 ID（范围：1-4）

默认设置

无

命令模式

特权 EXEC

例：

```
Switch#show spanning-tree ethernet 1/11
Bridge-group information
-----------------------------------------------------------------
 Spanning tree protocol           :IEEE Std 802.1D
 Spanning tree enable/disable     :enable
 Priority                         :40000
 Hello Time (sec.)                :5
 Max Age (sec.)                   :20
 Forward Delay (sec.)             :20
 Designated Root                  :40000.0030F1686740
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :0
 Last topology changes time (sec.):3417
 Hold times (sec.)                :1
------------------------------------------------------------------
Eth  1/11 information
-----------------------------------------------------------------
 Admin status             : enable
 STA state                : broken
 Path cost                : 100
 Priority                 : 128
 Designated cost          : 0
 Designated port          : 128.11
 Designated root          : 40000.0030F1686740
 Designated bridge        : 40000.0030F1686740
 Fast forwarding          : disable
 Forward transitions      : 0
Switch#
```

VLAN 命令

VLAN 是由位于网络中任何地方的一组端口组成的，但是它们可以像在同一网段中那样互相通信。这一节描述用来创建 VLAN 组，添加端口成员，规定 VLAN 标记的使用和为选定接口激活 VLAN 自动注册的命令。

vlan database

使用这个命令输入 VLAN 数据库的模式,这个模式下的所有命令立即生效。

默认设置

无

命令模式

全局配置

命令的使用

- 使用 VLAN DATABASE 命令模式来添加，改变和删除 VLAN。当更改配置后，你可以输入 SHOW VLAN 命令来显示当前设置。
- 使用 INTERFACE VLAN 命令模式来定义端口成员模式并从一个 VLAN 中添加或删除一个端口。这些命令的结果被写入运行配置文件，你可以输入 SHOW RUNNING-CONFIG 命令来显示这个文件。

例：

```
Switch(config)#vlan database
Switch(config-vlan)#
```

相关命令

SHOW VLAN

vlan

使用这个命令来配置一个 VLAN。使用 NO 的形式来恢复默认设置或删除一个 VLAN。

语法

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]

no vlan *vlan-id* [name | state]

- ◆ *vlan-id*——配置的 VLAN 的 ID
- ◆ name——VLAN 名字的关键字
  - ● vlan-name——1 到 32 个 ASCII 码字符
  - ● media Ethernet——以太网介质类型
  - ● state——VLAN 状态的关键字
    - -active——VLAN 是正在运行的
    - -suspend——VLAN 被延缓，这样的 VLAN 不传送数据包

默认设置

只有 VLAN1 是存在并运行的。

命令模式

VLAN 数据库配置

命令的使用

- 当命令 no vlan *vlan-id* 被使用，这个 VLAN 被删除。
- 当命令 no vlan *vlan-id* name 被使用，这个 VLAN 的名字被删除。
- 当命令 no vlan *vlan-id* state 被使用，这个 VLAN 返回默认的状态。
- VLAN1 不能被延缓，但是其他端口将被延缓。
- 可以在交换机上配置多达 127VLAN

例:

这个例子使用 VLAN-ID 105 和名字 RD5 来添加一个 VLAN。这个 VLAN 默认是激活的。

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 105 name 105 media ethernet
Switch(config-vlan)#
```

相关命令

SHOW VLAN

interface vlan

使用这个命令进入 VLAN 的接口配置模式，并且配置一个物理连接。

语法

interface vlan ***vlan-id***

***vlan-id*——配置的 VLAN 的 ID（范围：1-4094）**

默认设置

无

命令模式

全局配置

例:

下边的例子显示了怎样将接口配置模式设置为 VLAN 1，并且分配一个 IP 到 VLAN：

```
Switch(config-if)#ip address 192.168.1.254 255.255.255.0
Switch(config-if)#
```

相关命令

SHUTDOWN

switchport mode

使用这个命令为一个端口配置 VLAN 成员资格模式，使用 NO 的形式来恢复默认设置。

语法

switchport mode {**trunk** | **access**}

no switchport mode

- trunk——为一个 VLAN trunk 指定一个端口作为末点端口，一个 trunk 是两台交换机之间的直接连结，所以这个端口发送和接收区别源 VLAN 的加标记数据帧。
- access——设置端口作为未加标记的接口来操作。所有帧未加标记被发送。

默认的设置

所有的端口被设置为混合模式，设置 PVID 值为 VLAN 1。

命令模式

接口配置

命令的使用

这个命令与 switchport acceptable-frame-types 命令有着相同的效果。

例:

这个例子给端口 1 设置配置模式，然后设置交换端口为 trunk：

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

switchport acceptable-frame-types

使用这个命令来对端口配置可接收数据帧的类型，使用 NO 的形式来恢复默认设置。

语法

switchport acceptable-frame-types {all | tagged}

no switchport acceptable-frame-types

- **all——这个端口允许传送所有帧，包括加标记和未加标记的**
- **tagged——这个端口只接受加标记的帧**

默认设置

所有帧类型

命令模式

接口配置

命令的使用

- 当设置为接收所有的帧类型时，任意未加标记的、已接收的帧被分配到默认 VLAN。

例：

下边的例子显示了怎样限制端口 1 只能通过加标记的帧：

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport acceptable-frame-types tagged
Switch(config-if)#
```

switchport ingress-filtering

使用这个命令对一个端口激活进口过滤，使用 NO 的形式恢复默认设置。

语法

switchport ingress-filtering

no switchport ingress-filtering

默认设置

禁用

命令模式

接口配置

命令的使用

- **进口过滤只影响加标记的帧。**
- **如果进口过滤被禁用了，标记匹配 VLAN，那么接口将接受任意加 VLAN 标记的帧。（除非 VLAN 在这个端口上明确禁用）**
- **如果进口过滤被禁用了，流入的标记 VLAN 的帧如不包括这个进入端口，就会被丢弃。**
- **进口过滤不影响与于 BPDU 帧无关的 VLAN，例如 GVRP 或 STA。但是它们却能影响依赖 BPDU 帧的 VLAN，如 GMRP。**

例:

下边的例子设置了怎样为端口 1 设置接口，然后激活进口过滤：

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport ingress-filtering
Switch(config-if)#
```

switchport native vlan

使用这个命令为一个端口配置 PVID，使用 NO 的形式恢复默认值。

语法

switchport native vlan ***vlan-id***

no switchport native vlan

***vlan-id*——一个端口的默认 VLAN ID。（范围：1-4094）**

默认设置

VLAN 1

命令模式

接口配置

命令的使用

- **如果接口不是 VLAN 1 的成员，且你分配了它的 PVID 到这个 VLAN，**

那么接口将自动添加到 VLAN 1 作为一个未加标记的成员。对于其他 VLAN，在你分配接口的 PVID 到那个组之前，接口必须先配置为未加标记的成员。

- 如故可接受的帧类型被设为 all（所有），或交换机端口模式被设为 hybrid（混合），那么 PVID 将被插入到所有未加标记的帧，流入进入端口。

例:

下边的例子显示了怎样为端口 1 设置 PVID 给 VLAN 1。

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport native vlan 1
Switch(config-if)#
```

switchport allowed vlan

使用这个命令在选定的接口上配置 VLAN 组，使用 NO 的形式恢复默认值。

语法

switchport allowed vlan {**add** *vlan* | **remove** *vlan*}

no switchport allowed vlan

- **add** *vlan*——所要添加的 VLAN 标识符
- **remove** *vlan*——所要删除的 VLAN 标识符

默认设置

所有的端口被分配到 VLAN 1

帧类型未加标记

命令模式

接口配置

命令的使用

- 如果交换机端口模式设置为 TRUNK，那么你只能分配一个接口到 VLAN 组作为未加标记的成员。
- 帧总是在交换机中被加标记。加标记和未加标记的参数用于告知交换机是否从进口处的帧保留或除去标记。
- 如果链接的另一端所有媒质网络设备和主机都不支持 VLAN,那么应该添加接口到这些 VLAN 作为未加标记的成员。否则，有必要最多只添加一个 VLAN 作为未加标记的成员，这应该符合本地 VLAN。
- 如果手动添加禁用列中的 VLAN 到那个接口,那么 VLAN 自动从列中被删除。

例:

下边的例子显示了如何为端口 1 添加 VLAN 1，2，5 和 6 到加标记 VLAN：

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport allowed vlan add 1 tagged
Switch(config-if)#switchport allowed vlan add 2 tagged
Switch(config-if)#switchport allowed vlan add 5 tagged
Switch(config-if)#switchport allowed vlan add 6 tagged
Switch(config-if)#
```

switchport forbidden vlan

使用这个命令来配置禁止的 VLAN，使用 NO 的形式来删除禁止的 VLAN 列。

语法

switchport forbidden vlan {**add** *vlan* | **remove** *vlan*}

no switchport forbidden vlan

- **add *vlan*——所要添加的 VLAN ID**
- **remove *vlan*——所要删除的 VLAN ID**

默认设置

没有 VLAN 被包含在禁止 VLAN 列中。

命令模式

接口配置

命令的使用

- 这个命令防止了一个 VLAN 通过 GVRP 被自动添加到一个指定的接口中去。
- 如果 VLAN 已经添加到允许的 VLAN 中，那么对于同一个接口来说，你就不能添加它到禁止的 VLAN。

例:

这个例子显示了怎样防止端口 1 被添加到 VLAN105 中去：

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport forbidden vlan add 105
Switch(config-if)#
```

show vlan

使用这个命令来显示 VLAN 信息。

语法

show vlan [id *vlan-id* | name *vlan-name*]

- ◆ **id**——VLAN ID 的关键字
  - -*vlan-id*——配置的 VLAN 的 ID（范围：1-4094）
- ◆ **name**——VLAN 名字的关键字
  - - *vlan-name*——ASCII 字符串从 1 到 32 个字符

默认设置

显示所有 VLAN

命令模式

普通 EXEC，特权 EXEC

例:

下边的例子说明了怎样显示 VLAN 1 的信息：

```
Switch#show vlan id 1
VLAN Type     Name               Status    Ports/Channel groups
---- -------- ---------------- --------- ----------------------------------------
   1  Static       DefaultVlan      Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
                                           Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
                                           Eth1/11 Eth1/12 Eth1/13 Eth1/14 Eth1/15
                                           Eth1/16 Eth1/17 Eth1/18 Eth1/19 Eth1/20
                                           Eth1/21 Eth1/22 Eth1/23 Eth1/24 Eth1/25
                                           Eth1/26
Switch#
```

私有 VLAN 命令

私有 VLAN **提供基于端口的安全性和端口间的隔离。本款交换机支持两种类型的私有** VLAN **端口：混合端口和共同端口。混合端口能在私有** VLAN **中的所有接口间通信。共同端口只能和在其他端口自己的共同** VLAN **中和这些端口通信，并和指定的混合端口通信。这一节讲述了用于配置私有** VLAN **的命令。**

请按以下步骤配置私有 VLAN**：**

1. **使用private-vlan命令指定一个多多个共同**VLAN**和主要**VLAN**，这些**VLAN**会引导数据流流出共同组**
2. **使用private-vlan association命令映射次要**VLAN**（例：共同**VLAN**）到主要**VLAN
3. **使用switchport mode private-vlan命令配置端口作为混合（例：能访问所有主要**VLAN**中的端口）或主机（例：能访问受限的共同**VLAN**成员并引导所有的其他数据流通过混合端口）**
4. **使用switchport private-vlan host-association命令分配端口到次要**VLAN

5. **使用switchport private-vlan mapping命令分配端口到主要**VLAN
6. **使用show vlan private-vlan命令检验你的配置设置**

pvlan

使用这个命令创建主要或次要私有 VLAN。使用 NO 的形式删除指定的私有 VLAN。

语法

private-vlan *vlan-id* {**community** | **primary**}

no private-vlan *vlan-id*

- *vlan-id*——**私有**VLAN**的**ID（**范围：**2-4094）
- **community**——VLAN**中的数据流受到端口成员的限制**
- **primary**——VLAN**能包含一个或多个共同**VLAN**并服务于引导共同**VLAN**和其他地方的数据流。**

默认设置

无

命令模式

VLAN 配置

命令的使用

- **私有 VLAN 用于限制同一个 VLAN “团体”中的端口数据流。**
- **私有 VLAN 的端口成员资格是静态的。一旦端口已经分配到私有 VLAN，它就不能通过 GVRP 被动态移到另一个 VLAN。**
- **私有 VLAN 端口不能设置为 TRUNKED 模式。（参看本章节“switchport mode”）**

例：

```
Switch(config)#vlan database
Switch(config-vlan)#private-vlan 2 primary
Switch(config-vlan)#private-vlan 3 community
Switch(config-vlan)#
Switch(config-vlan)#
```

private vlan association

使用这个命令将主要 VLAN **和次要** VLAN **建立关联。使用** NO **的形式断开所有的关联。**

语法

private-vlan *primary-vlan-id* **association** {*secondary-vlan-id* |
add *secondary-vlan-id* | **remove** *secondary-vlan-id*}

no private-vlan *primary-vlan-id* **association**

- *primary-vlan-id*——**主要**VLAN **的**ID（**范围**：2-4094）
- *secondary-vlan-id*——**次要**VLAN **的**ID（**范围**：2-4094）

默认设置

无

命令模式

VLAN 配置

命令的使用

次要 VLAN 对组成员提供安全性。被关联的主要 VLAN 提供普通界面访问主要 VLAN 中（例：配置了混合端口的服务器）的其他网络资源，并访问主要 VLAN 以外的资源（通过混合端口）。

例：

```
Switch(config-vlan)#private-vlan 2 association 3
Switch(config-vlan)#
```

switchport mode private-vlan

使用这个命令对接口设置私有 VLAN 模式。使用 NO 的形式恢复默认设置。

语法

switchport mode private-vlan {**host** | **promiscuous**}

no switchport mode private-vlan

- **host——此端口能和分配到同一个次要VLAN中所有其他主机端口进行通信。这个VLAN以外的所有通信必须通过次要VLAN的混合端口。**
- **promiscuous——此端口类型能和同一主要VLAN中所有的其他混合端口进行通信，也能和被关联的次要VLAN中所有的端口进行通信。**

默认设置

普通 VLAN

命令模式

接口配置

命令的使用

分配到主要 VLAN 的混合端口能和同一个 VLAN 中的所有其他混合端口进行通信，也能和被关联的次要 VLAN 中所有的端口进行通信。

例：

```
Switch(config)#interface ethernet 1/2
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#exit
Switch(config)#interface ethernet 1/3
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#
```

switchport private-vlan host-association

使用这个命令对次要 VLAN 和接口产生关联。使用 NO 的形式断开关联。

语法

switchport private-vlan host-association *secondary-vlan-id*

no switchport private-vlan host-association

secondary-vlan-id——次要VLAN的ID（范围：2-4094）

默认设置

无

命令模式

接口配置

命令的使用

所有分配到次要 VLAN 的端口能通过组成员间的数据流，但是必须通过混合端口和组以外的资源进行通信。

例：

```
Switch(config)#interface ethernet 1/3
Switch(config-if)#switchport private-vlan host-association 3
Switch(config-if)#
```

switchport private-vlan mapping

使用此命令映射接口到主要 VLAN。**使用 NO 的形式除去映射。**

语法

switchport private-vlan mapping *primary-vlan-id*

no switchport private-vlan mapping

- *primary-vlan-id*——主要VLAN的ID（范围：2-4094）

默认设置

无

命令模式

接口配置

命令的使用

分配到主要 VLAN 的混合端口能和同一 VLAN 中的任意其他混合端口进行通信，也能和任意被关联的次要 VLAN 中的组成员进行通信。

例：

```
Switch(config)#interface ethernet 1/2
Switch(config-if)#switchport private-vlan mapping 2
Switch(config-if)#
```

show vlan private-vlan

使用这个命令显示交换机上的私有 VLAN **配置设置。**

语法

show vlan private-vlan [**community** | **primary**]

- **community——显示所有的共同**VLAN**、它们的主要**VLAN**和被分配的主机接口**
- **primary——显示所有的主要**VLAN**和任意被分配的混合接口**

默认设置

无

命令模式

特权 EXEC

例：

```
Switch#show vlan private-vlan
Primary   Secondary      Type       Interfaces
--------  -----------  ----------  ----------------------------------
     2                 primary    Eth1/ 2
     2         3       community Eth1/ 3
Switch#
```

GVRP 和桥路扩展命令

GVRP VLAN 注册协议定义了一个方法使得交换机能够交换 VLAN 信息，从而使得网络接口能自动注册 VLAN 成员。这一节描述了怎样为单个的接口和全局的为交换机激活 GVRP,怎样显示桥路扩展 MIB 的默认配置信息。

switchport gvrp

使用这个命令为一个端口激活 GVRP，使用 NO 的形式禁用它。

语法

switchport gvrp

no switchport gvrp

默认设置

禁用

命令模式

接口模式

命令的使用

GVRP只能对标记的端口激活。你必须设置switchport mode为TRUNK，以便配置一个加标记的端口。

例：

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#switchport gvrp
Switch(config-if)#
```

相关命令

switchport mode

show gvrp configuration

使用这个命令来显示 GVRP 是否被激活。

语法

show gvrp configuration [*interface*]

interface

- 以太网 *unit*/*port*
  - -*unit*——设备 1
  - -*port*——端口号
- **port-channel**——通道 ID

默认设置

显示全局和指定接口的配置

命令模式

普通 EXEC，特权 EXEC

例：

```
Switch#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 Gvrp configuration: Disabled
```

garp timer

使用这个命令为加入，离开，离开所有设置计时器，使用 NO 的形式恢复默认数值。

语法

garp timer {join | leave | leaveall} *timer_value*

no garp timer {join | leave | leaveall}

- {join | leave | leaveall}——被设置的计时器
- *timer_value*——计时器的数值

默认设置

加入：20 秒

离开：6 秒

离开所有：100 秒

命令模式

接口配置

命令的使用

- 组地址注册协议是被 GVRP 和 GMRP 用来在一个桥路局域网中为客户

服务注册或是取消注册客户属性的。GARP 计数器是与介质接入方式与数据速率相独立的，除非你在 GMRP 或 GVRP 注册或取消注册是遇到了困难，否则这些数据是不应该被改变的。

- 计时器的数值被应用于所有 VLAN 的所有端口的 GVRP 中。
- 计时器的数值必须受到下列限制：

—leave >= (3 x join)

—leaveall > leave

注意：在同一个网络中的 2 层设备 GVRP 计时器应该被设置为同一数值。

例：

```
Switch(config)#interface ethernet 1/1
Switch(config-if)#garp timer join 100
Switch(config-if)#
```

相关命令

show garp timer

show garp timer

使用这个命令为选择的接口显示 GARP 计时器。

语法

show garp timer [*interface*]

interface

- 以太网 *unit/port*
  - -*unit*——设备 1
  - -*port*——端口号
- **port-channel**——通道 ID

默认设置

显示所有 GARP 计时器

命令模式

普通 EXEC，特权 EXEC

例：

```
Switch#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer: 20 centiseconds
 Leave timer: 60 centiseconds
 Leaveall timer: 1000 centiseconds
```

相关命令

GARP TIMER

bridge-ext gvrp

使用这个命令来激活 GVRP，使用 NO 的形式来禁止它。

语法

bridge-ext gvrp

no bridge-ext gvrp

默认设置

禁用

命令模式

全局配置

命令的使用

GVRP 为交换机提供了一种方法在网络中为了注册在端口上的 VLAN 成员而交换信息。这个功能应该被激活以允许自动的 VLAN 注册，并且

支持扩展当地交换机的 VLAN。

例：

```
Switch(config)#bridge-ext gvrp
Switch(config)#
```

show bridge-ext

使用这个命令来为桥路扩展命令显示配置。

默认设置

无

命令模式

特权 EXEC

命令的使用

参看本章中的“ Displaying Basic VLAN Information” **和**“ Displaying Bridge Extension Capabilities”**获取显示项的详细描述。**

例：

```
Switch#show bridge-ext
 Max support vlan numbers: 127
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: SVL
 Configurable PVID tagging: Yes
 Local VLAN capable: No
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Switch#
```

优先级命令

在本节描述的命令在由于数据拥挤数据存储在交换机的缓冲器中时，允许你规定哪一种的数据有着更大的优先权。这个交换机在每个端口支持有着 4 个优先权队列的 COS。一个端口中有着比较大的优先权的数据将在较小优先权的数据之前被传送。你可以为每一个接口设值默认的优先权。

queue mode

使用这个命令给 4 种服务级别的优先权队列分配加权循环。使用 NO 的形式恢复默认设置。

语法

queue mode {**strict** | **wrr**}

no queue mode

- **strict**——按照次序，服务出口队列，在服务低优先级队列前，以高优先级发送所有的数据流。
- **wrr**——通过分别分配 WRR 权 1，3，12，48 给 COS 优先权队列 0，1，2，3，加权循环在出口端口共享带宽。

默认设置

加权循环

命令模式

全局配置

例：

下边的例子设置队列模式为严格优先级模式：

```
Switch(config)#queue mode strict
Switch(config)#
```

show queue mode

使用这个命令显示当前队列模式。

默认设置

无

命令模式

特权 EXEC

例:

```
Switch#show queue mode

Wrr status: Disabled
Switch#
```

镜像端口命令

这一节描述怎样从一个源端口向一个目的端口镜像数据流。

port monitor

使用这个命令配置一个镜像会话，使用 NO 的形式来清除一个镜像会话。

语法

port monitor *interface* [**rx** | **tx** | **both**]

no port monitor *interface*

- **rx**——映像接收的数据包

◆ **tx**——映像发送的数据包

◆ **both**——映像接收和发送的数据包

默认设置

没有映像会话被定义，当激活后，默认的镜像既针对接收的数据包又针对发送的数据包。

命令模式

接口配置

命令的使用

- 你可以从任何的源端口镜像流量到目的端口以进行实时的分析。
- 目的端口是通过规定一个以太网接口来设置的。

例:

下边的例子显示了如何配置交换机将所有端口 6 的数据包镜像到端口 11：

```
Switch(config)#interface ethernet 1/11
Switch(config-if)#port monitor ethernet 1/6 both
Switch(config-if)#
```

show port monitor

使用这个命令显示镜像信息。

语法

show port monitor [*interface*]

默认设置

显示所有的会话

命令模式

特权 EXEC

命令的使用

此命令显示当前配置的源端口，目的端口和镜像模式（例 :RX，TX，RX/TX）

例:

下边的例子显示了从端口 6 到端口 11 的镜像配置：

```
Switch(config)#interface ethernet 1/11
Switch(config-if)#port monitor ethernet 1/6
Switch(config-if)#end
Switch#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/11
 Source port(monitored port)  :Eth1/ 6
 Mode                         :RX/TX

Switch#
```

端口聚合命令

端口能够静态的被组合成一个集合连结来增加网络连结的带宽或者确保故障恢复。或者你可以使用连结集合控制协议自动的在交换机和另外一台网络设备间创建一个 trunk 连结。你可以在相同类型的交换机之间配置 trunk。所有的交换机必须符合 CISCO 以太网信道标准。本款交换机最多支持 4 个 trunk。例如，一个由两个 1000MBPS 端口组成的 trunk，当用全双工模式操作时，它能支持 4GBPS 的集成带宽。

port-group

使用这个命令添加一个预先确定的端口到trunk。使用NO的形式从trunk除去端口组。

语法

port-group *port-group-number*

no port-group

port-group-number——组成员（范围：1-10）

组成员	端口
1	1
2	1-2
3	1-4
4	5
5	5-6
6	5-8
7	9
8	9-10
9	9-12
10	25-26

默认设置

无

命令模式

接口配置

命令的使用

使用no channel-group从TRUNK**除去一个端口组**

使用no interfaces port-channel从交换机除去一个TRUNK

例：

本例创建TRUNK1**并添加端口**1**和**13。

```
Switch(config)#interface port-channel 1
Switch(config-if)#port-group 1
Switch(config-if)#
```

附录 A 疑难解答

常见故障

1． **无法使用 Telnet，Web 浏览器和 SNMP 进行连接。**

- **确定已经给代理配置了有效的 IP 地址，子网掩码和默认网关**
- **确定管理站点拥有可以访问交换机的管理 VLAN（默认为 VLAN 1）**
- **检查和交换机的连接正确，所使用的端口没有禁用**
- **检查网线**
- **如果无法使用 Telnet，可能因为超过了同时允许的 Telnet 会话的最大数，稍候再连接**

2． **不能通过控制口访问内置的配置程序。**

- **将终端模拟程序设置为 VT100 兼容，8 个数据位，1 个停止位，无奇偶，9600bps**
- **检查 null-modem 串行线符合附录 B 的管脚分配**

3． **忘记密码**

- **重装交换机的操作代码。直接连到控制口，对交换机通电。自检时，访问固件下载菜单，选择合适的项。**

通过串口升级固件

交换机由两个可以升级的部件——诊断代码（BOOT-ROM）和操作代码。升级操作代码可以通过 RS-232 串口，连接 TFTP 服务器和 SNMP 管理软件。诊断代码只能通过 RS-232 串口升级。

注意：你可通过 TFTP 使用 Web 界面下载操作代码。下载大的操作代码

文件时，使用 TFTP 比串口快。

你也可以将 PC 连到串口上，通过支持 XModem 的终端仿真程序，升级固件。

1 将 PC 连到控制口，使用 null-modem 或带有母 DB-9 连接头的 RS-232 交叉线。

2 配置终端仿真程序，8 个数据位，1 个停止位，无奇偶，9600 波特，流量控制无

3 对交换机通电。

4 初始化界面出现时，在诊断测试结束后立刻按<ESC>键。

```
[1]Image Update
[2]System Parameters
[3]Change Baud rate
[4]Do all the following Test
[5]Testing the System SDRAM
[6]MPC 850 internal clock Timer and Interrupt Test
[7]WATCHDOG Timer and Interrupt Test
[8]ACD chip Test
[9]Switch Loopback Test
[G]oto System
ReB[O]ot Again
Enter Selection:
```

5 按<3>，改变串行连接的波特率。

6 按<5>，选择 115200 波特。

7 提供你 5 个波特率：9600，19200，38400，57600，115200。使用最高的波特率以减少下载固件代码文件的时间。

```
Enter Selection: 3
Change main console baudrate :
[0] Quit
[1] 9600   bps
[2] 19200  bps
[3] 38400  bps
[4] 57600  bps
[5] 115200 bps
```

8 设置 PC 的终端效法固件匹配 115200 波特率。按回车重设交换机通信。

9 按<1>开始下载新的代码文件。

10 如果使用 Windows 的超级终端，点"Transfer"，"Send file…"，选择 Xmodem 协议。用"Browser"选择需要的固件代码，Xmodem file send 窗口会显示下载过程。

注意：下载的必须是二进制文件。

11 下载后，提示你"Update Image File"，让你指定代码类型。<r>代表运行时间代码，<d>代表诊断代码。

12 指定代码名字，最多 32 个字符，区分大小写，不含空格。

13 例如：以下界面文本显示运行时间代码文件的下载过程：

```
Image download at Baudrate [115200]. Please Change your setting
Xmodem Receiving Start ::
Image downloaded to buffer.

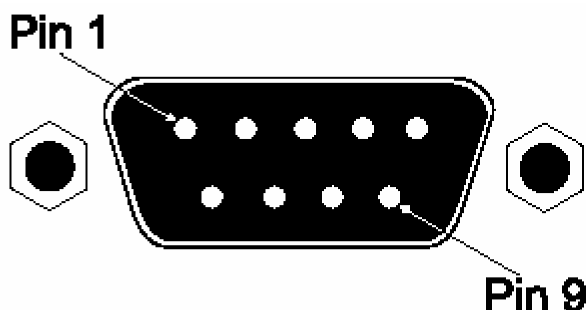

        [R]untime
        [D]iagnostic
        [L]oader (Warning: you sure what you are doing?)
Update Image File:r
Runtime Image Filename : acd
Updating file system.
File system updated.
Please change your Baudrate to default then press any key to continue
```

14 **设置** PC **终端效法软件的波特率为** 9600**。按回车重设交换机通信。**

附录 B 管脚分配

控制口管脚分配

交换机后面板上的 DB-9 串口管脚用于把交换机和管理设备连接。主板上的配置程序能被终端、运行终端模拟程序的 PC 或通过调制解调器建立的远程连接访问到。你可以通过管理端口配置端口，或升级设备固件。管脚分配用于把各种类型的设备与下表提供的交换机管理端口向连接。



DB9 端口管脚分配

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #
BB	104	RxD (Received Data)	2	2
BA	103	TxD (Transmitted Data)	3	3
AB	102	SGND (Signal Ground)	5	5

控制台口对 PC 的 9 针 DTE 端口

Switch's 9-Pin Serial Port	Null Modem	PC's 9-Pin DTE Port
2 RXD	<---------TXD ------------	3 TXD
3 TXD	-----------RXD ---------->	2 RXD
5 SGND	-----------SGND ----------	5 SGND

控制台口对 PC 的 25 针 DTE 端口

Switch's 9-Pin Serial Port	Null Modem	PC's 25-Pin DTE Port
2 RXD	<---------TXD ------------	2 TXD
3 TXD	-----------RXD ---------->	3 RXD
5 SGND	-----------SGND ----------	7 SGND